PRIVACY POLICY AND NOTICE

Last Revised: 27 October 2025

Contents

1. WHO IS RESPONSIBLE FOR PROCESSING YOUR DATA AND HOW TO CONTACT US?

This Privacy and Data Protection Policy and Notice ("**Notice**") describes the steps the Telit Cinterion group (collectively, "**Telit Cinterion**", "**we**", "**our**", or "**us**") take to protect the personal data that we process about our customers, partners and other business-related personal data.

We are committed to the protection of your personal data in accordance with the data protection principles set out in the European Union's ("**EU**") General Data Protection Regulation 2016/679 (which has been incorporated into United Kingdom ("**UK**") law in a substantially similar form) ("**GDPR**"), the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020) and its implementing regulations ("**CCPA"**) and other applicable data protection laws. In respect of certain personal data that is collected or otherwise processed as part of the services and products that we

offer (see Section 2.2 (personal data related to the services and products that we offer) below), the Data Controller (as defined under the GDPR) or business (as defined under the CCPA) in respect of your personal data is the entity with which your employer has a contractual relationship with for the provision of those services and products. The Data Controller(s) in respect of all other processing activities outlined in this Notice is, depending on the context, any/all of the Telit Cinterion entities provided here as Annex 1 below. If you are unsure which entity is the Data Controller in respect of your personal data, you may contact us by using the following email address: privacy@telit.com. Please note we maintain a separate privacy notice concerning the processing of the personal data of our employees.

2. WHAT PERSONAL DATA WE COLLECT AND WHY?

We may source, use, and otherwise process your personal data in different ways. In all cases, we are committed to protecting the personal data that we process. In each of the sub-sections listed below, we describe how we obtain your personal data and how it is handled by us.

In some cases, we are legally required to collect and process certain personal data (for example, to comply with tax, bookkeeping, employment, anti-money-laundering, or export control obligations). In other cases, providing your personal data is voluntary. However, if you choose not to provide information that is necessary for us to respond to your request, deliver our services, or consider you for employment, we may be unable to do so.

2.1 Representatives of our Existing or Prospective Customers, Distributors, Subcontractors and Vendors

Sources of Personal Data

We may obtain your personal data from various sources, including: directly from you when you provide it through means such as our website's lead collection forms, subscribing to our newsletters or webinars, registering to our online technical documentation portal (the "**Download Zone**"), contacting us via phone or email, or participating in webinars, networking events, or exhibitions that we host, sponsor, or attend, including when you provide your business card or have your badge scanned at such events. Additionally, we may collect personal data when you seek support or provide feedback on our services and products, such as through customer satisfaction surveys. We may also receive your personal data from your employer, if they are a customer, vendor, or partner of ours, or from other business partners with whom we have a relationship. Furthermore, we may obtain data from publicly available sources, such as your employer's website or social media platforms, as well as from other third parties, including credit reference agencies, financial institutions, bodies involved in anti-money laundering compliance, export control compliance, and third party contact list vendors.

Personal Data that We Collect and Process

We may collect personal data related to employees, officers, authorized signatories, and other individuals associated with our existing and prospective customers, distributors, subcontractors, vendors and other business partners. This may include details such as personal names, employer information, job title, country and business contact details like

addresses, email addresses and telephone numbers. Additionally, we may collect the contents of correspondence, including mail and emails, exchanged with these individuals. This information is gathered to perform marketing outreach and to establish and manage business relationships and communications effectively.

When you register to our Download Zone, you provide us with the above details, in addition to your area of interest in our services and products and login credentials to the Download Zone. The data you provide in this context is used to verify your identity, provide you with secure access to the Download Zone and present you with tailored content and updates as relevant to your area of interest in our services and products, such as user guides, application notes, product change notices, software and firmware releases.

For the purposes of fulfilling anti-money laundering and export control compliance requirements, we may collect personal data from individuals associated with the business, such as principals, executives, or key stakeholders. This data may include identifying details such as full name, date of birth, and address, as well as nationality and residency status. We may also gather documentation to verify identity and address, such as passports, driver's licenses, utility bills, and bank account information. In some cases, we may collect additional data such as tax identification numbers, proof of business ownership, or legal records, including police contact certificates, when required by law. All data is collected to ensure compliance with regulatory obligations and to verify the legitimacy of the business relationship.

As part of our creditworthiness assessments for prospective clients, we may collect and process certain information about the entity and, where necessary, individuals associated with the business, such as principals, executives, or key stakeholders. This information may include, but is not limited to, full names, ID numbers, title, date of appointment to present position, contact details, year of birth, education details and qualifications, as relevant to assess the financial stability of the business. We may also obtain reports from credit reference agencies or financial institutions. All information collected is used solely to evaluate the business's ability to meet its financial obligations.

The aforementioned types of personal data we collect correspond to the following categories of personal information collected by us and disclosed for business purposes within the past 12 months in our role as a "business" (as defined in the CCPA) or as a "controller" (as defined in other US state privacy laws):

- Identifiers and information that relates to, describes, or is capable of being associated with, a particular individual;
- Professional or employment-related information; and
- Commercial information, including products or services purchased, obtained, or considered.
- Sensitive personal information (as defined under the CCPA or other applicable US state privacy laws): government-issued IDs, financial account information and contents of mail and email.

Why Do We Collect Your Personal Data and What are the Lawful Bases?

Purpose for Processing of Your Personal Data	Lawful Basis for Processing of Your Personal Data	Our Legitimate Interest in the Processing of Your Personal Data / Additional Details
Providing you with our products or services or receiving products or services from you; managing our business relationship with you	Performance of contract; legitimate interests	Efficiently fulfil our contractual obligations, account management, exercising or defending against legal claims, market evaluation, management reporting (including at an intra-group level)
Providing our Download Zone	Legitimate Interests; Consent (for receiving Download Zone updates)	Verifying your identity and providing you with secure access to the Download Zone, presenting you with content and updates as relevant to your area of interest in our services and products
Assessing the financial stability of our clients	Legitimate Interests	Ensuring the business's ability to meet its financial obligations
Sending you customer satisfaction surveys, increasing internal awareness and analytics about how our products and services may be used in order to maintain and improve our services and products	Legitimate Interests	Understanding the market in which we operate, product and customer satisfaction improvement, account management and management reporting (internally and externally)
Security management	Legitimate Interests	Ensuring the security of our products and services, risk and crime prevention, management reporting (internally and externally)
Marketing communications: establishment and management of our business relationship with you by increasing your awareness about products, services, and events that may be of interest to you through marketing communications by letter, phone, email, or other forms of electronic communication	Legitimate Interests or Consent* (according to applicable law)	Promoting our products and services, establishment, maintenance and management of our business relations, management reporting (internally and externally)
General business management	Legitimate Interests	Management reporting and assessments
Compliance with legal obligations	Legal Obligation	Reporting to applicable bodies/entities as required by law, compliance with other legal obligations (e.g. tax laws,

		bookkeeping laws, anti-money laundering laws, export control compliance regulation, etc.)

* Certain direct marketing purposes may be based on your consent (if required by law). For example, when you submit a 'contact us' form directly to our sales, analyst relations or media relations teams, inquire about our products and services, provide us your business card or badge for scanning purposes or contact us following an event. Sometimes, we rely on the consent you've provided to third parties to receive marketing communications from companies like ours. If we've relied on consent, you are entitled to withdraw your consent at any time.

We may also rely on our legitimate interests to contact you in order to offer you services or products similar to the ones you have bought from us, requested an offer, or inquired about, or to invite you to future events of a similar nature to the one you've registered to.

If you object to our use of your personal data for the aforementioned purposes, including for direct marketing purposes, please contact us by using the following email address: privacy@telit.com. You can also unsubscribe from our marketing communications by emailing unsubscribe@telit.com.

We will seek your prior consent, when required by applicable law, when, for direct marketing purposes, we use (a) cookies or other similar tracking technologies, and/or (b) your email address to communicate marketing information to you.

The following are the CCPA business or commercial purposes for which we use the categories of personal information included under this section:

- Auditing related to a current interaction with the consumer and concurrent transactions.
- Providing customer service, processing or fulfilling orders and transactions, verifying customer information.
- Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us.
- All information, including sensitive personal information, is used only as necessary to perform our services, provide our products and conduct our business operations, and is not sold or shared.

2.2 Personal Data Related to the Services and Products We Provide

Sources of Personal Data

Your personal data may be processed by us when our customers or their customers use the services and/or products that we provide, including, but not limited to, the following (to the extent the data being processed via these services and/or products relates to you):

- Connectivity – a cloud-based management platform for cellular connectivity (SIM) services provided to customers.
- IoT Platform (deviceWISE/IoT Portal) and related Professional Services – a cloud-based solution that allows customers to connect an array of IoT devices and handle data collected by these devices.
- IoT Suite – a remote eSIM management solution which allows customers to remotely manage cellular network operator subscriptions by allowing them to provision so-called operator profiles into an eSIM throughout the lifecycle of the IoT devices through a dedicated web portal.
- Fleet Manager – a cloud-based remote IoT fleet management web portal, based off of the IoT Suite, which allows customers to store and manage activation codes by means of configurable business rules.
- Support Services (Pre-Sales and Post-Sales) – technical support activities relating to our SaaS solutions, which may include demonstrations, proof-of-concepts, troubleshooting and resolving customer cases, and which may involve access to prospect and customer environments.

Personal Data that We Collect and Process

We collect the following categories of personal data as part of providing our services and products:

1. **Customer User Data:** data related to the authorized users of our services on behalf of our customers or customers' customers ("Customer Users"), including, as applicable:
   (i) Account Data: account login credentials (email, password), name (first and last), work title, company name, country, phone number;
   (ii) Activity Log Data: logs of Customer User activity within the applicable service, such as logins, event and activity timestamps and descriptions, file downloads.
2. **IoT Device End User Data:** highly pseudonymized data relating to customers' (or customers' customers') end-users of the IoT devices connected to certain Telit Cinterion solutions ("End Users"), to the extent such End Users are natural persons.

For clarification, Telit Cinterion is an IoT company specializing in M2M (machine-to-machine) solutions. We do not sell our products or services to End Users, but rather to corporate customers across various industries including medical, energy and agriculture. Our customers, or our third party providers' (e.g. Mobile Network Operators) and underlying platforms' (e.g. Connected Device Platforms) customers integrate our solutions and products into their IoT devices and machinery for operational purposes.

Given our business model, we do not receive or process directly identifying data of End Users (such as names or contact details) and we cannot reasonably identify such individuals in any way based on the data processed through our services. However, we acknowledge that in certain circumstances - particularly where IoT devices are used consistently by small groups of individuals - our customers may be able to link some datapoints to specific persons. Regardless, we do not process End User data for the purpose of identifying individuals, and it is the sole determination of our customers whether to utilize this data for such purposes.

End User data may be applicable to the following services, as follows:

- Connectivity Data: data related to the cellular connectivity of modules, associated SIM cards or virtual eSIMs embedded in IoT devices and machines, such as module, SIM, subscription and network identifiers, transmission metadata, and technical content data.
- IoT Platform (deviceWISE/IoT Portal) and related Professional Services: data related to the IoT devices managed by Telit Cinterion's IoT Platform. In certain circumstances, certain (e.g., geolocation or usage history of an assigned device) may indirectly relate to individuals, especially in assigned-use or small fleet contexts.
- IoT Suite Data: data related Telit Cinterion's remote eSIM management solution, such as network identifiers (e.g., SIM or device IDs), transmission and connection metadata, and associated location information.
- Fleet Manager Data: data related Telit Cinterion's fleet management solution, such as configuration data, connectivity and operation metadata, and customer-provided content or labels.

The aforementioned types of personal data we collect from you correspond to the following categories of personal information collected by us within the past 12 months and disclosed for business purposes in our role as a "business" (as defined in the CCPA defined below):

- Identifiers and information that relates to, describes, or is capable of being associated with, a particular individual; and
- Professional or employment-related information.

Why Do We Collect Your Personal Data and What are the Lawful Bases?

Purpose for Processing of Your Personal Data	**Lawful Basis for Processing of Your Personal Data**	**Our Legitimate Interest in the Processing of Your Personal Data/ additional information**
Providing our services	Processing under the DPA (we act as processor on the customer's instructions)	Processing of data necessary for the operation of the services
Billing and account administration	Legitimate interests (ensuring accurate invoicing and enforcing agreements); Legal obligation (retaining tax and accounting records)	Includes usage metadata required for invoicing, as well as retention of invoices, receipts, and other financial records as required by applicable law.
General business management	Legitimate Interests	Conducting administrative and technical activities necessary to maintain and improve our services, exercise or defend legal claims
Providing Support Services (Pre-Sales and Post-Sales)	Pre-sales: Legitimate interests (controller role). Post-sales: Processing under the DPA (processor role).	For pre-sales: delivering efficient technical support to enable prospects to evaluate our services and facilitating the establishment of a commercial relationship.

		For post-sales: ensuring proper performance of our contractual obligations, limited to processing carried out under the customer's instructions pursuant to the DPA.
Ensuring the performance and security of our services	Legitimate Interests	Providing secure access to the services, preventing fraud, misappropriation, infringements, identity theft or misuse of the services
Statutory reporting obligations	Legal obligation	Report to relevant bodies or entities where required by law

The following are the CCPA business or commercial purposes for which we use the categories of personal information included under this section:

- Auditing related to a current interaction with the consumer and concurrent transactions.
- Providing customer service and technical support, including pre-sales demonstrations, proof-of-concepts, and post-sales troubleshooting; processing or fulfilling orders and transactions, verifying customer information.
- Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us.

We note that certain End User datapoints processed as part of our services are processed by us as a Data Controller, as this data is necessary to ensure accurate invoicing and billing for our services. This data includes module, SIM, subscription and network identifiers as well as certain transmission metadata.

The remaining End User data under this section, such as Content Data and certain transmission and operation metadata (cell ID location, GPS location, device IP address and associated logs), in addition to Customer User Data, are processed by us as a Data Processor on behalf of our customers, who are the Data Controllers of such data pursuant to the GDPR and other applicable laws. As such, our customers are responsible to determine the lawful basis and purposes for the processing of such data. Similarly, when processing such data, we are merely a 'service provider' of our customer pursuant to the CCPA.

2.3 Visitors to our Premises

Sources of Personal Data

We may obtain your personal data from (a) you directly, and/or (b) from our systems' records

Personal Data that We Collect and Process

Your (a) name, (b) business contact details, (c) organization, (d) job title, and/or (e) image(s) (for example, from CCTV cameras at some of our premises).

The aforementioned types of personal data we collect from you correspond to the following categories of personal information collected by us within the past 12 months and disclosed for business purposes in our role as a "business" (as defined in the CCPA defined below):

- Identifiers and information that relates to, describes, or is capable of being associated with, a particular individual; and
- Professional or employment-related information.

Why Do We Collect Your Personal Data and What are the Lawful Bases?

Purpose for Processing of Your Personal Data	Lawful Basis for Processing of Your Personal Data	Our Legitimate Interest in the Processing of Your Personal Data
Security management	Legitimate Interests	Security management and risk and crime prevention
Maintaining records of visitors to our premises	Legitimate Interests	Management reporting and risk management
Statutory reporting obligations	Legal obligation	Report to relevant bodies or entities where required by law

If you object to our use of your personal data for the aforementioned purposes, please contact us by using the following email address: privacy@telit.com.

The following are the CCPA business or commercial purposes for which we use the categories of personal information included under this section: Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity and prosecuting those responsible for such activity.

2.4 Website Visitors

Sources of Personal Data

We may obtain your personal data from (a) your device and browser, whenever you visit our website (b) you directly, for example, when you complete the contact forms on our website, subscribe to our newsletter via our website, post content and comments on our Technical Forum, etc.

Personal Data that We Collect and Process

Your (a) name, (b) business inquiry, (c) email address, (d) phone number, (e) address, (f) company name, (g) job title, (h) operating system, (i) browser type, (j) device information, (k) viewed or searched products or services, (l) other website data, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page, (m) cookie data (for more information about our use of cookies, please see our Cookie Notice at www.telit.com/cookie-policy), (n) list of website pages visited by you with timestamps, (o) IP address.

The aforementioned types of personal data we collect from you correspond to the following categories of personal information collected by us and disclosed for business purposes within the past 12 months in our role as a "business" (as defined in the CCPA):

- Identifiers and information that relates to, describes, or is capable of being associated with, a particular individual;

- Professional or employment-related information;
- Commercial information, including products or services purchased, obtained, or considered;
- Device and browser information;
- General geolocation data;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application or advertisement.

Why Do We Collect Your Personal Data and What are the Lawful Bases?

Purpose for Processing of Your Personal Data	**Lawful Basis for Processing of Your Personal Data**	**Our Legitimate Interest in the Processing of Your Personal Data**
Establishment and management of our relationship with you	Legitimate Interests	Efficiently fulfilling our contractual and legal obligations, providing support, exercising or defending against legal claims, market evaluation, management reporting (internally and externally)
Increasing internal awareness about how our products, services and website may be used	Legitimate Interests	Understanding the market in which we operate, improving our website and presenting its contents to you, management reporting (internally and externally)
Security management	Legitimate Interests	Security management and risk and crime prevention, including anti-money laundering, export control compliance, and management reporting (internally and externally)
Increasing your awareness about products, services, and events that may be of interest to you by letter, phone, email, or other forms of electronic communication	Legitimate Interests	Promoting our products and services
General business management	Legitimate Interests	Management reporting and assessments
Statutory reporting obligations	Legal Obligation	Reporting to applicable bodies/entities as required by law

If you object to our use of your personal data for the aforementioned purposes, including for direct marketing purposes, please contact us by using the following email address: privacy@telit.com.

We will seek your prior consent, when required by applicable law, when, for direct marketing purposes, we use (a) cookies or other similar technologies, and/or (b) your email address to communicate marketing information to you.

The following are the CCPA business or commercial purposes for which we use each category of personal information. Details about the information we collect for each category are provided above.

Categories of Personal Information	Business or Commercial Purposes Pursuant to the CCPA
Identifiers and information that relates to, describes, or is capable of being associated with, a particular individual; professional or employment-related information.	Performing services, including providing customer service, verifying customer information. Auditing related to a current interaction with the consumer who is a job applicant.
Device and browser information, Internet or other electronic network activity information	Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity and prosecuting those responsible for such activity. Improving our website and presenting its contents to you. Undertaking internal research for technological development and demonstration. Conducting business analysis, such as analytics, projections, identifying areas for operational improvement. Undertaking activities to verify or maintain the quality of the service and to improve, upgrade, or enhance the service. Debugging to identify and repair errors.

2.5 Whistleblowing Procedures

Sources of Personal Data

We may obtain your personal data from (a) you directly, for example, when you submit a whistleblower report through our internal reporting channel or through external reporting channels (such as designated authorities), and/or (b) another individual who submitted a whistleblower report referencing you through our internal reporting channel or through external reporting channels.

Personal Data that We Collect and Process

Whistleblower data: Telit Cinterion provides a fully anonymous internal whistleblowing reporting channel. If you decide to remain anonymous as a reporter by using this channel, we will not have access to your identity. However, please be aware that, depending on the content of the report, it may be possible to draw conclusions about your identity. Also, if you don't provide us with your contact details, we will not be able to provide you with feedback regarding your report.

If you choose to report using your identity, we will process your (a) name, (b) email address (c) employee number (to the extent you are our employee), and (d) any other personal information you choose to provide in the report. Please note that reported information is handled confidentially. Within the scope of applicable laws (such as the EU Whistleblower Protection Directive (Directive (EU) 2019/1937) the identity of the reporting person will not be disclosed to anyone beyond authorized staff members who are competent to receive or follow-up on reports, unless explicit consent is provided by the reporting person or where it is necessary and proportionate under applicable laws (such as EU or Member State law), particularly in the context of investigations by national authorities or judicial proceedings. This does not apply to persons reporting false information willfully or in gross negligence. If necessary to engage external expertise (e.g., legal and auditing services), we may forward personal data to such parties.

Other data: We will also process personal data of accused individuals, witnesses or other data subjects included in whistleblowing allegations, as contained in whistleblowing reports submitted to us and in the documentation and evidence collected during the investigations of such procedures, including data collected from our information systems, as well as any other personal data required in order to manage such procedures.

For further information please see our Whistleblowing Policy.

The aforementioned types of personal data we collect correspond to the following categories of personal information collected by us and disclosed for business purposes within the past 12 months in our role as a "business" (as defined in the CCPA) or as a "controller" (as defined in other US state privacy laws):

- Identifiers and information that relates to, describes, or is capable of being associated with, a particular individual;
- Professional or employment-related information; and
- Sensitive personal information (as defined under the CCPA or other applicable US state privacy laws): contents of mail and email.

Why Do We Collect Your Personal Data and What are the Lawful Bases?

Purpose for Processing of Your Personal Data	**Lawful Basis for Processing of Your Personal Data**	**Our Legitimate Interest in the Processing of Your Personal Data / additional details**
Processing required by applicable whistleblower laws (e.g. EU Whistleblower Protection Directive and corresponding national laws) and statutory reporting obligations	Legal Obligation	
Management of whistleblowing procedures, when the processing is not	Legitimate Interests	Investigating misconduct, effectively enforcing whistleblower compliance standards and requirements,

required under applicable laws		Internal business process optimization, exercising or defending legal rights
Disclosing the identity of the reporting person (when such disclosure is not a statutory obligation)	Explicit consent	Identity of reporting person is disclosed to a controlled and limited set of parties for the purpose of the investigation, such as internal investigation team, senior management and external legal counsel
Processing special category data	Public Interest (if applicable) or explicit consent	

2.6 Job Applicants

Sources of Personal Data

When you apply to a position at Telit Cinterion, you provide us with your personal data. Please note that, in most cases, we receive the information directly from you (such as through our website career portal, mail or email), or record data in interview records, but we may also receive information from recruitment service providers and consultants, online professional networks (e.g. LinkedIn), references or background check companies. This information is necessary to initiate, carry out or terminate the application process, to exercise and fulfill legal and contractual obligations and, if necessary, for the purpose of legal prosecution. If you do not provide us with this data, we will not be able to assess you as a candidate and advance your recruitment process.

Personal Data that We Collect and Process

When you apply for a job with us, we may collect and process the following personal data:

- **Basic Information**: Your name, contact details, and gender.
- **Employment Details**: Employment history, education background, qualifications, training, certifications, skills, and any other relevant information included in your resume (C.V.) and job application.
- **Application Insights**: Desired salary expectations, personal characteristics (e.g., reliability), career priorities (e.g., opportunities for advancement, job preferences), availability, preferred start date, and type of desired employment.
- **Correspondence and References**: Email communications, information from references, and notes from job interviews.
- **Assessment and Background Checks**: Responses to assessments (such as integrity tests) and results from background checks, as permitted by applicable law.

In certain situations, we may also collect special categories of personal data, including national origin, citizenship status, health information (e.g., disability status, pregnancy), and gender identity. If you apply through our website career portal, we will also gather technical data, including your IP address, the destination URL, the content of your request, and the access status or HTTP status code.

The aforementioned types of personal data we collect from you correspond to the following categories of personal information collected by us and disclosed for business purposes within the past 12 months in our role as a "business" (as defined in the CCPA):

- Identifiers and information that relates to, describes, or is capable of being associated with, a particular individual, such as your name, contact information and gender;
- Professional or Employment-Related Information: This includes your skills, employment history, education, qualifications, and training, professional experience, salary expectations, career priorities, availability, and job preferences;
- Sensitive Personal Information: As defined under the CCPA and applicable state privacy laws, this includes government-issued IDs, health data, and other sensitive information you may provide;
- Technical Data: Information collected from our website career portal, such as IP address, browsing history, device information, and access status or HTTP status codes.

Why Do We Collect Your Personal Data and What are the Lawful Bases?

Purpose for Processing of Your Personal Data	**Lawful Basis for Processing of Your Personal Data**	**Our Legitimate Interest in the Processing of Your Personal Data/ other details**
Carrying out the recruitment and employment evaluation process	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (in conjunction with GDPR Article 9(2)(b) for special category data)	Evaluating employment candidates, digital processing of application, communication with applicants, obtaining background checks and references, recruitment tests.
Processing and temporary storage of website access logs	Legitimate Interest	To secure our information technology systems, ensure the functionality and security of our website and enable the delivery of the website to your end device
To comply with our legal obligations as an employer (e.g. to check your eligibility to work), to respond to legal	Legal obligation	

proceedings, subpoenas or inquiries from supervisory authorities or other competent authorities		
Legal prosecution	Legitimate interest	To enforce our own legal claims or defend ourselves against legal claims
Adding your details to our applicant pool	Consent	Retaining your data on a long-term basis for future vacancies

The following are the CCPA business or commercial purposes for which we use the categories of personal information included under this section:

- Auditing and evaluation related to a current interaction with the applicant.
- Determine the terms of employment offer.
- Complete background checks.
- Comply with and enforce applicable legal and regulatory obligations.
- All information, including sensitive personal information is used only as necessary to conduct our business operations in relation to the job application process, and is not sold or shared.

3. WHO DO WE SHARE YOUR PERSONAL DATA WITH?

Summary: we share personal data with our service providers, partners, group companies, and authorities, where required.

Affiliates

We may share your personal data internally with our affiliated companies to the extent necessary to fulfill the purposes listed above in Section 2 ('what personal data we collect and why?'), including our business representatives or of any of our affiliated companies, whether wholly or partially owned by us or co-owned companies. Sharing your personal data will always take place under an approved transfer mechanism, such as the relevant standard contractual clauses, if applicable.

Our Service Providers

We transfer personal data to third parties under a variety of circumstances. We endeavor to ensure that such third-party recipients use your personal data only to the extent necessary to perform their functions and to have an agreement in place with them to govern such processing on our behalf. These third parties include business partners, suppliers, affiliates, agents and/or sub-contractors for the performance of any agreement we enter into with you or with your employer. They assist us in providing the services and products we offer, processing transactions, fulfilling requests for information, receiving and sending communications, analyzing data, providing IT and other support services, and other tasks from time to time. These third parties may also include analytics and search engine providers that assist us in the improvement and optimization of our websites and for marketing purposes.

We periodically add and remove third-party service providers. At the present time, we may share your information with the following types of service providers:

- our distributors in your area who distribute Telit Cinterion's products and services, and who may contact you to offer Telit Cinterion's products and services;
- technical support providers who assist with our website and IT infrastructure;
- third party software providers, including 'software as a service' solution providers, where the provider hosts the relevant personal data on our behalf;
- professional advisers such as legal consultants, accountants, tax advisors, debt collection agencies, auditors and insurance brokers;
- providers that help us generate and collate reviews in relation to our products and services;
- our advertising and promotional agencies and consultants and those organizations selected by us to carry out marketing campaigns on our behalf; and/or
- providers that help us store, collate and organize information effectively and securely, both electronically and in hard copy format (e.g. cloud service providers), and for marketing purposes.

Content that you post on Telit Cinterion's Technical Forum may be viewable by other users of the website and Internet users in general, along with your username on the website. For the avoidance of doubt, we may transfer and disclose non-personal data to third parties at our own discretion.

Mergers and Acquisitions

We may disclose your personal data to third parties if some or all of our companies or assets are acquired by a third party, including by way of a merger, share acquisition, asset purchase, or similar transaction in which personal data will be one of the transferred assets.

Protection of Rights, Compliance and Legal and Regulatory Obligations

We will transfer your personal data to third parties if we are under a duty to disclose or share such data (a) in order to comply with any legal, auditory, or compliance obligation, (b) in the course of any legal or regulatory proceeding or investigation, (c) in order to enforce or apply our terms and other agreements with you or with a third party, or (d) in order to assert or protect our rights, property, or safety or those of others. This includes exchanging information with other companies and organizations for the purposes of complying with our legal and regulatory obligations, asserting or protecting our rights, fraud protection, credit risk reduction, and the prevention of cybercrime.

4. WHERE DO WE STORE YOUR DATA?

Summary: we store your personal data across multiple global locations.

We store your personal data on servers owned or controlled by us or have such data processed by third parties on behalf of us, such as by reputable cloud service providers (see Section 5 (transfers of personal data outside the EU/European Economic Area) regarding international transfers).

5. INTERNATIONAL TRANSFERS OF PERSONAL DATA

Summary: we transfer personal data internationally, including to and from the EEA, UK, US, Israel, China, Taiwan, Japan, Australia, South Korea, Brazil and elsewhere with appropriate safeguards in place.

We transfer personal data internationally in order to:

- Store or backup the information;
- Enable us to fulfill our contractual commitments to you or your employer;
- Enable us to fulfill any legal, auditory, ethical, or compliance obligations which require us to make such a transfer;
- Facilitate the operation of our group business, where it is in our legitimate interest, and we have concluded that such interest(s) are not overridden by your right(s);
- Serve our shareholders across multiple jurisdictions; and
- Operate our affiliates in an efficient and optimal manner.

Transfers from EU/UK: Your personal data may be transferred to, stored, and processed at a location outside of the European Economic Area ("**EEA**") and the UK. We will only do so using one of the following safeguards:

a.) the transfer is to a non-EEA country (or non-UK country) that has been the subject of an adequacy decision by the European Commission or by the UK (as applicable);

b.) the transfer is covered by a contractual agreement, which covers the GDPR requirements relating to transfers to countries outside the EEA/UK, such as the Standard Contractual Clauses ("**SCCs**") published by the European Commission or the UK's International Data Transfer Addendum to the EU Commission;

c.) the transfer is to an organization which has binding corporate rules approved by an EU or UK, data protection authority; or

d.) the transfer is to an organization in the US that is EU-US Privacy Shield certified.

International transfers to our affiliates, subsidiaries and parent company are governed by applicable Standard Contractual Clauses for Controllers and, where relevant, for Processors.

We may also transfer your data to third-party vendors outside the EU/UK, such as our customer relationship management (CRM) system and due diligence providers (e.g., Salesforce and Amazon Web Services (AWS)). Where we do so, the SCCs or other safeguards are in place to safeguard that personal data.

For more information about these safeguards, please contact us by using the following email address: privacy@telit.com.

Transfer of personal Data from P.R. China: Personal data originating from the People's Republic of China (P.R. China) may be transferred to locations outside P.R. China only under certain circumstances. These circumstances include conducting an internal assessment of the receiving entity and its safeguards and ensuring compliance with applicable laws of P.R. China regarding the outbound transfer of personal data.

6. YOUR RIGHTS (EEA/UK/SWITZERLAND/OTHER APPLICABLE LOCATIONS)

Summary: depending on the law applicable to your personal data, you may have various data subject rights, such as rights to access, erase, and correct your personal data, in addition to information rights. We will respect any lawful request to exercise those rights.

If the GDPR (or other applicable data protection laws) applies to the processing of your personal data, subject to the circumstances and legal exemptions that may apply, you have certain rights in relation to the processing of your personal data by us as a controller. These rights may vary depending on your location and applicable laws, and may include the rights to:

- **Access** – the right to request confirmation that personal data about you is being processed by us and, if so, what types and for what purposes, as well as for how long and with whom your personal data is being shared with. This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Rectification** – the right to request correction or updating to any of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Erasure** – the right to request the deletion of any personal data about you held by us.
- **Portability** – the right to request that any personal data about you held by us be transferred to you or any third party in a machine-readable formatted copy.
- **Restriction of Processing** – the right to request that your personal data held by us cease being processed. This may be exercised to allow the accuracy of such data to be confirmed or while you evaluate a legal basis for processing.
- **Objection** – the right to object to the processing of your personal data by us under certain circumstances. This right may apply where the processing of your personal data is based on our legitimate interests (including for direct marketing), as explained above, or where decisions about you are based solely on automated processing, including profiling.
- **Withdrawal of Consent** – the right to withdraw your consent at any time to our processing of your personal data where such processing relies on your consent. For example, if we collected your consent to receive our marketing communications, you can also unsubscribe from such communications by emailing unsubscribe@telit.com.

If at any time you decide that you would like to exercise any of your rights as set out above, you can contact us by emailing the following email address: privacy@telit.com. We will respond to such requests without undue delay as required by applicable law. Please note that we may have to undertake an authentication process prior to facilitating the exercise of any requested right(s). Furthermore, please note that personal data held by us may be either deleted or retained in an aggregated manner without being linked to any personal identifiers depending on specific technical and commercial capabilities. Such data may continue to be processed by us.

Please note that these rights only apply under certain circumstances and may be limited by law, as well as subject to exceptions. For example, where accepting your request to exercise a right would adversely affect other individuals, expose our trade secrets or intellectual property, where there are overriding public interests, or where we are required by law to retain your personal data. In addition, such rights cannot be exercised by data subjects in a manner inconsistent with the rights of our staff or third-party rights. For example, job references, reviews, internal notes and assessments, documents and notes, including proprietary information or other forms of intellectual property, cannot be accessed, erased, or rectified by data subjects. In addition, these rights may not be exercisable where they relate to data that is not in a structured form, such as emails, or where other exceptions apply.

Data subjects in the EU, the UK and other jurisdictions have the right to lodge a complaint with a local data protection supervisory authority. If such authority fails to respond to such a complaint, the applicable data subject may have the right to an effective judicial remedy.

7. YOUR RIGHTS AND ADDITIONAL DISCLOSURES (U.S. STATES, INCLUDING CALIFORNIA, VIRGINIA, COLORADO, CONNECTICUT, UTAH, TEXAS, IOWA, MONTANA, INDIANA, DELAWARE, OREGON, NEW JERSEY, NEW HAMPSHIRE)

Summary: We share limited website user data with third parties for online advertising and analytics purposes. California and other US state consumers have certain rights in relation to their personal information. They may exercise such rights by contacting us.

This section provides additional details about the personal information we collect about consumers in California, Virginia, Colorado, Connecticut, Utah, Texas, Iowa, Montana, Indiana, Delaware, Oregon, New Jersey, New Hampshire and other applicable US states and the rights afforded to them under the CCPA and other applicable US state privacy laws.

Subject to certain limitations, if you are a resident of one of the US states mentioned above, or of other states with applicable privacy laws, you have the following rights in relation to personal information we process about you (other than processing personal information as a service provider of a corporate customer):

- **Access** - The right to know what personal information we have collected about you, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom we disclose personal information, and the specific pieces of personal information the we have collected about you. This may also include under certain laws the right to obtain the personal information in a portable and, to the extent technically feasible, readily usable format.
- **Delete** - The right to delete personal information that we have collected from you, subject to certain exceptions.
- **Correct** - The right to correct inaccurate personal information that we maintain about you.
- **Opt Out of Sale or Sharing of Personal Information** - The right to opt-out of the sale or sharing of your personal information, including from the use of your personal information for cross-contextual behavioral advertising, targeted advertising (as defined by applicable laws) or certain types of profiling. Please note we do not engage in such types of profiling of individuals.
- **Limit Use of Sensitive Information** - If we use or disclose sensitive personal information for reasons other than standard business purposes (such as purposes set forth in section 7027, subsection (m) of the California Consumer Privacy Act Regulations), the right to limit the use or disclosure of your sensitive personal information. Please note we do not use sensitive personal information for such purposes.
- **Non-discrimination** - The right not to receive discriminatory treatment by us for the exercise of privacy rights conferred by applicable laws.

If you would like to exercise any of your rights as described above, you should email us to: privacy@telit.com. We may ask you for additional information to confirm your identity and for security

purposes before disclosing the personal information requested by you, such as by using a two-or three-point data verification process, depending on the type of information being requested. If we refuse your request, you may have the right to appeal our decision using the same email address described above. You may also designate an authorized agent to make a request on your behalf. To do so, you need to provide the authorized agent written permission to do so and the agent will need to submit to us proof that they have been authorized by you.

For details about personal information that we have collected as a business and disclosed for business purposes over the last 12 months, please see Section 2 ('what personal data we collect and why?') above. We share this information with the categories of third parties described in Section 3 ('who do we share your personal data with?') above. In the last 12 months, we have not sold or shared any personal information, aside from website visitor information, as described in the next paragraph ('Notice of Right to Opt-out of Sale/Sharing'). We do not use or disclose sensitive personal information for reasons other than standard business purposes, such as the purposes set forth in section 7027, subsection (m) of the California Consumer Privacy Act Regulations. We do not knowingly or willingly share or sell (for cross-contextual behavioral advertising or targeted advertising purposes) data of users under 16 years of age.

Notice of Right to Opt-out of Sale/Sharing

We do not sell your personal information in the conventional sense, such as for monetary gain. However, like many companies, we use advertising and analytics services that are intended to analyze your interactions with our website, based on information obtained from cookies or other trackers as further described in detail in our Cookie Policy. Please note that these activities constitute "sharing" and "selling" website visitor information (as described under Section 2 above) with third parties for the purpose of cross-context behavioral advertising (as defined in the CCPA), targeted advertising (as defined in other applicable US state laws) and website analytics purposes. Such third parties consist of analytics, marketing and search engine providers that assist us in the improvement and optimization of our websites and for marketing purposes. If you are a resident of California, Virginia, Colorado, Utah, Connecticut, Texas, Iowa, Montana, Indiana, Delaware, Oregon, Indianna and other applicable jurisdictions, you may opt out of the sharing or selling of your data for such purposes by clicking here, or within our Cookie Storage Preferences tool (located by clicking the floating cookie icon to the bottom left of the web page) by switching the toggle under "Do Not Sell or Share My Personal Information" to the right and clicking save. This signal will apply to your browser and device in a frictionless manner. If you switch browsers or devices you will need to opt-out again. You may also set the Global Privacy Control (GPC) to opt out of the "sale" or "sharing" of your personal information for targeted advertising for each participating browser system that you use.

8. RETENTION PERIOD

Summary: we retain your personal data according to our data retention policy, as required to meet our obligations, protect our rights, and manage our business.

We will keep and process your personal data only for as long as is necessary for the purposes for which it was collected in connection with your relationship with us, unless we have a legal right or obligation to retain the data for a longer period, or the data is necessary for the establishment, exercise or defense of legal claims or the enforcement of agreements. This includes retaining your personal data in order to meet any audit, compliance and business best-practices obligations.

Your personal data that is no longer needed to be retained will be anonymized or deleted. For example, metadata or statistical information that are not subject to deletion pursuant to this policy may be retained but it will be impossible to identify you from this data. Lastly, some data may be retained on the servers of our third-party service providers until deleted pursuant to their applicable policies, as well as in our back-up drives until overwritten.

9. SECURITY AND STORAGE OF INFORMATION

Summary: we take data security very seriously, invest in security systems, and train our staff in data security procedures. In the event of a breach, we will notify the appropriate individuals as required by law.

We take great care in implementing, enforcing and maintaining the security of the personal data we process. We implement, enforce, and maintain security measures, technologies, and policies to prevent the unauthorized or accidental access to or destruction, loss, modification, use, or disclosure of personal data. We likewise take steps to monitor compliance of such policies on an ongoing basis. Where we deem it necessary in light of the nature of the data in question and the risks to data subjects, we encrypt data. Likewise, we maintain cybersecurity standards that exceed industry standards to ensure our website and platforms are safe.

Please note, however, that no data security measures are perfect or impenetrable, and we cannot guarantee that unauthorized access, leaks, viruses and other data security breaches will never occur.

Within Telit Cinterion, we endeavor to limit access to personal data to those of our personnel who: (i) require access in order for us to fulfil our obligations, including also pursuant to our agreements, and as described in this Notice; (ii) have been appropriately and periodically trained with respect to the requirements applicable to the processing, care and handling of the personal data; and (iii) are under confidentiality obligations as may be required under applicable law.

We shall act in accordance with our policies and with applicable law to promptly notify the relevant authorities and data subjects in the event that any personal data processed by us is lost, stolen, or where there has been any unauthorized access to it, all in accordance with applicable law and on the instructions of qualified authority and we shall promptly take reasonable remedial measures.

10. GENERAL

Children Under 16. We do not knowingly collect or solicit information or data from or about children under the age of 16 or knowingly allow children under the age of 16 to register for our services. If you are under the age of 16, do not register or attempt to register for any of our services or send any information about yourself to us. If we learn that we have collected or have been sent personal data from a child under the age of 16, we will delete that personal data as soon as reasonably practicable without any liability to us. If you believe that we might have collected or been sent information from a minor under the age of 16, please send an email immediately to privacy@telit.com.

Changes to this Notice. The terms of this Notice will govern the use of the services, websites, and any information collected in connection with them. We may amend or update this Notice from time to time. The most current version of this Notice will be available at: https://www.telit.com/privacy-policy/. Changes to this Notice are effective as of the stated "Last Revised" date above and your

continued use of our services will constitute your active acceptance of the changes to and terms of the Notice.

Contact Us. We aim to process only adequate, accurate and relevant data limited to the needs and purposes for which it is gathered. We also aim to store data for the time period necessary to fulfill the purpose for which the data is gathered. We only collect data in connection with a specific lawful purpose and only process data in accordance with this Notice. For any questions, complaints or comments concerning this Notice, you are welcome to contact us (details below) and we will make an effort to reply within a reasonable timeframe.

Our Data Protection Officer (DPO) may be contacted at: privacy@telit.com.

Our details are as follows:

Telit IoT Solutions Holding Ltd. (or other Telit Cinterion entities and branches as listed in Annex 1 below)

Cannon Place, 78 Cannon Street, London, England, EC4N 6AF

ANNEX 1: TELIT CINTERION ENTITIES AND BRANCHES

EU ENTITIES

TELIT ENTITY	**COUNTRY**
Telit Communications SpA	Italy
Telit Wireless Solutions GmbH	Germany
Telit Cinterion Deutschland GmbH	Germany
Telit Communications Spain SL	Spain
Telit Communications Cyprus Ltd.	Cyprus
Telit Technologies (Cyprus) Ltd.	Cyprus
Telit IoT Solutions Filial (Branch)	Sweden
Telit Wireless Solutions Gmbh (Branch)	France

ENTITIES OUTSIDE THE EU

TELIT ENTITY	**COUNTRY**
Telit IoT Solutions Holding Ltd.	United Kingdom
Telit IoT Solutions Ltd.	United Kingdom

Telit IoT Ltd.	United Kingdom
Telit Communications Limited	United Kingdom
Telit IoT Solutions, Inc.	United States
Telit Wireless Solutions Tecnologia E Serviços Ltda	Brazil
Telit Cinterion Brasil Ltda	Brazil
Telit Wireless Solutions Co Ltd	Republic of Korea
Telit Wireless Solutions Ltd.	Israel
Telit Wireless Services Ltd.	Israel
Telit Wireless Solutions Hong Kong Limited	Hong Kong
Telit Wireless Solutions (Australia) Pty Limited	Australia
Telit Wireless Solutions (Shenzen) Ltd.	China
Telit Wireless Solutions (Shanghai) Ltd.	China
Telit Wireless Solutions (Shanghai) Ltd. Beijing Branch office	China
Telit Wireless Solutions (Shanghai) Ltd. Dalian Branch office	China
Telit Wireless Solutions Japan KK	Japan
Telit Wireless Solutions Taiwan Limited	Taiwan
Telit Communications India Private Limited	India