Lusha's Privacy Practices

White Paper

Version 5.0 - Aug, 2026

Table of Contents:

1 Our Privacy Statement

At Lusha, protecting the privacy of our customers and data subjects is of the utmost importance to us: we are committed to data protection and being transparent about our data practices.

We don't just say it; we do it. Lusha's privacy and security practices are audited annually by impartial third parties so that you can rest assured that we, as your data vendor, are compliant and can be trusted. Below is a summary of Lusha's certifications.

<table>
<tr>
<td>Lusha is the only data broker with an <u>Accredited</u> ISO 27701 Certification
<u>Privacy Information Management</u>
ISO 27701
Trust Lusha to process personal data in compliance with international privacy standards</td>
<td>Lusha is the only data broker audited and granted with ISO 31700 Certification.
<u>Privacy by Design</u>
Trust that Lusha will not sell its customers' data
(also written in the agreement)</td>
<td>Lusha is the only data broker audited and certified by European auditors as
<u>GDPR Compliant</u>
ePrivacyseal
Trust Lusha's processes to be compliant with GDPR and German law</td>
</tr>
<tr>
<td colspan="2">Lusha is among the only data brokers who have both an AI certification:
<u>ISO/IEC 42001</u> and <u>TRUSTe Responsible AI</u>
Responsible AI ISO/IEC 42001
Trust Lusha's industry-leading Artificial Intelligence Management System (AIMS) and compliance program</td>
<td>Lusha is among the few data brokers that have validated its
<u>CCPA compliance.</u>
Trust Lusha's processes to be compliant with the CCPA/CPRA</td>
</tr>
<tr>
<td>SOC2 Type2
Trust that Lusha's internal controls and systems uphold the highest level of information security</td>
<td>ISO 27001
Trust that Lusha's ISO 27001 certification demonstrates the highest information security standards</td>
<td>Cloud Security Alliance STAR 1
Trust that Lusha's CSA STAR certification demonstrates top-tier security, transparency, and accountability.</td>
</tr>
</table>

Lusha is an IAPP member committed to ensuring that its *<u>legal and compliance team members are IAPP-certified</u>*

Trust Lusha's privacy team to handle privacy issues with great care

2 Professional in-house privacy team

2.1 Lusha's dedicated privacy and compliance team ensures that Lusha remains at the forefront of legislative and regulatory developments and the implementation of responsible AI. Along with the security, product, engineering, development, and sales teams, they work to ensure the highest standards of privacy protection for its customers and data subjects.

2.2 The majority of the members of its privacy, legal, and compliance teams have received certification as privacy professionals from the International Association of Privacy Professionals (IAPP).

2.3 Lusha's privacy and compliance team uses data guidance and first-tier law firms to monitor privacy legislation, regulations, and rulings. It also maintains robust and appropriate policies and practices which will be detailed hereunder.

2.4 Lusha maintains an IAPP corporate membership, which evidences its commitment to giving its team access to the privacy education, resources, and information they need to stay abreast of legal developments and manage data protection risks and challenges effectively.

2.5 Our Legal and Compliance team:

- General Counsel: David Kaplansky
- Director of Legal and Compliance: Assaf Gilad (CIPP/E, CIPP/US)
- Lead Legal Counsel: Diana Berkowitz (CIPP/E)
- Contracts Manager: Trix Neethling (CIPP/E)

To conclude, Lusha's Privacy, Legal, and Compliance team monitors global privacy regulations to ensure that its research and development practices comply with applicable laws.

3 Privacy landscape and its applicability to Lusha

3.1 Worldwide compliance status

3.1.1 To comply with ever-changing privacy regulations worldwide, Lusha has obtained ISO 27701 certification, which is the highest international standard for responsibility and transparency in the processing of personal information and was recognized by the CNIL (French data protection authority) as a key factor to evidence GDPR compliance.

Lusha was the first sales intelligence platform to receive ISO 27701 certification and is the only data broker that earned an accredited ISO 27701 certification which ensures data privacy practices have been thoroughly and independently validated by a recognized accreditation body (Certificate attached hereto as Annex E).

3.1.2 Lusha has been certified by ePrivacy (a German state-certified auditor) as GDPR Compliant (and German law-compliant). With respect to our customers who are subject to the GDPR, Lusha satisfies all the requirements to act as a lawful processor and comply with the GDPR (Certificate attached hereto as Annex B).

3.1.3 Lusha also validates its compliance with the CCPA through an audit conducted by TrustArc, providing you with the assurance that Lusha's privacy policies and practices meet the Privacy and Data Governance Practices of California law (Validation Letter attached hereto as Annex D). Lusha is a duly registered data broker in California, Vermont, Oregon, and Texas.

3.1.4 Some of our customers may be subject to the GDPR, CCPA, or other regional privacy laws. While the GDPR serves as the gold standard for international privacy laws, on request, with respect to certain additional jurisdictions, Lusha can provide evidence or other assurances necessary to demonstrate its compliance with these and other applicable privacy laws. From time to time, Lusha will publish on its website articles in response to data protection authorities' publications in its Trust Center (e.g., compliance with Dutch regulator guidelines).

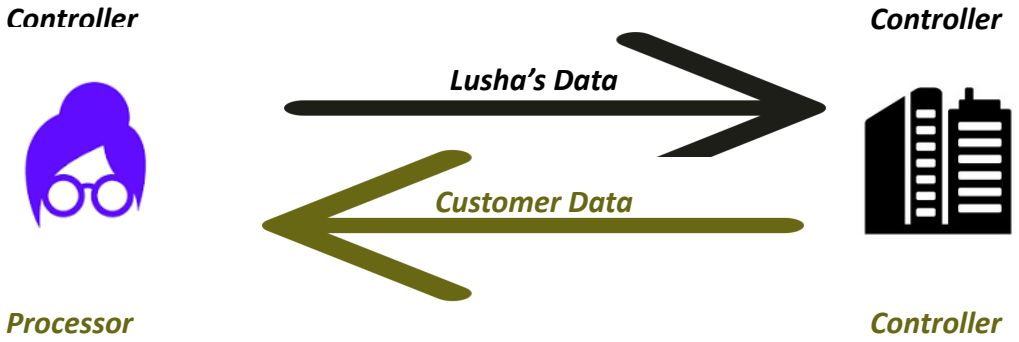
For more information, visit our Trust Center.

To conclude, Lusha's processes comply with international standards, EU/UK GDPR and CCPA. To confirm this, Lusha undergoes third-party international audits on an annual basis.

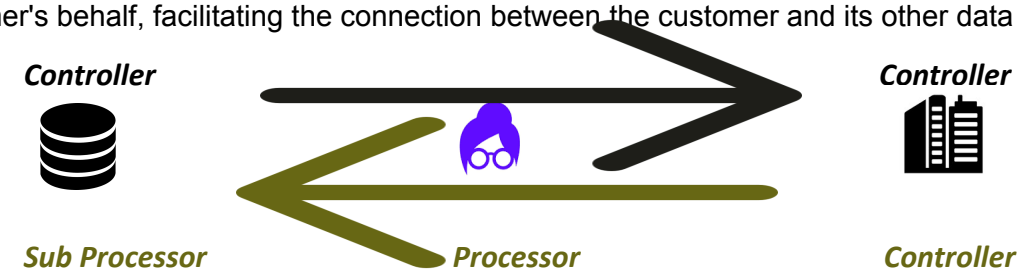
3.2 Lusha's role in processing data

Independent Data Controllers: Customers decide independently how and why they process personal data. For data sold or transferred *from* Lusha to customers, both parties act as independent data controllers. This independent relationship is explicitly set out in our Data Processing Agreement (DPA).

Data Processor ("Service Provider"): When a customer provides employee details (names and emails) to provision end-user accounts or utilizes CRM enrichment integrations, Lusha acts strictly as a data processor. In this capacity, Lusha processes data solely under the customer's explicit instructions.



Recently, Lusha introduced the "waterfall" service, when Lusha's own data does not return a match for a given query, the Waterfall Services will query the Customer's enabled Waterfall Providers to attempt to locate a result. In this case, Lusha acts solely as a processor on the customer's behalf, facilitating the connection between the customer and its other data vendors.



To conclude, Personal Data sent by our customers to Lusha will be processed in our capacity as a Processor ("Service Provider" under the CCPA) of our customer, who is the Data Controller of such data. Whereas, Personal Data transferred to our customers from Lusha will be governed by an independent controller-independent controller relationship.

When using other data providers within the Lush platform, Lusha acts as a Processor.

3.3 Data Transfers

3.3.1 Lusha bases its international data transfer on the SCCs, as approved by the EU Commission, to establish a lawful transfer of data. These are incorporated by reference in our customer DPA, which is available here.

3.3.2 Our DPA contains terms that ensure the confidentiality of your data and incorporate data protection obligations consistent with applicable privacy laws. For a list of third-party subprocessors, including their purpose, locations, and transfer mechanism, see here. Lusha has also signed DPAs and NDAs with all of its subprocessors.

3.3.3 Other than the subprocessors mentioned above, Lusha processes its customer data in Israel (a country with an adequate level of data protection, as determined by this EU Commission adequacy decision) and in the US (by the Lusha US sales team). To assist you with completing a Transfer Impact Assessment with respect to use of our Platform, we have prepared this TIA for your reference.

3.3.4 As an additional service will offer soon (for an extra cost), the ability to exclude the processing of your data in the EU. You can ask your sales representative about this "EU data residency service"; however, please note that in such an event, your sales and support representatives will only be available Monday to Friday from 2:00 AM to 5:00 PM (ET), and from 8:00 AM to 5:00 PM (ET) on Sundays.

3.3.5 Lusha has implemented the Government Data Access Policy. Lusha is committed to implementing and maintaining a solid and privacy-preserving procedure for reviewing and responding to any subpoena, warrant, or other judicial, regulatory, governmental, or administrative order, proceeding, demand, or request (whether formal or informal) by a government or quasi-governmental or other regulatory authority (including law enforcement or intelligence agencies) seeking or requiring access to or disclosure of Personal Data

To conclude, Lusha's customers can trust Lusha to handle their personal data with the highest level of confidentiality and integrity, not utilize their data for purposes other than for providing the services, and process their data in accordance with an adequate level of data protection.

3.4 Legal basis for the processing of professional business contact information

3.4.1 While consent is one basis for lawful processing under global privacy laws, it is not the only one. Consent is one of six lawful bases for the processing of data (seeArticle 6(1)(f) of the GDPR). Lusha's legal basis for the processing of personal information is legitimate interest (i.e., providing its services to its customers). Lusha's database is compiled from various sources, including publicly available sources, and contributor programs of Lusha and its affiliates (such as the Community Program). All data collected from our data sources is added to Lusha's data lake, where Lusha's proprietary algorithm organizes, scans, and merges certain data attributes into a unique identifiable "Business Contact Card," which is located in a highly secure database ("**B2B Database**"). These Business Contact Cards consist of individuals' professional information that is generally provided on business cards or is often displayed on company websites or in email signatures.

3.4.2 Lusha collects business contact information and other data associated with business professionals who choose to publish their business persona on a publicly available webpage (e.g. on their own firm website, public LinkedIn page) to enhance freedom to operate and market access and to help our customers facilitate more business transactions with minimal time and effort.

3.4.3 In accordance with certain privacy regulations (similar to Art 14 of the GDPR), Lusha implemented processes to inform the data subjects that Lusha holds their personal information. This notice provides the data subjects with the option to opt out within 14 days before adding the individual information to our user-facing database. Sample wording of such a notice, in multiple languages, is available here

3.4.4 With the help of first-tier law firms, Lusha conducted a Data Privacy Impact Assessment ("**DPIA''**) and Legitimate Interest Assessment ("**LIA**") that has reached the conclusion that Lusha's processing of Business Contact Cards satisfies the legitimate interest grounds for processing and is not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. A summary of the DPIA and LIA. available upon request to existing customers or once an NDA is in place.

To conclude, Lusha processes business contact information based on legitimate interest, not consent, in compliance with GDPR, and accordingly, Lusha sends a privacy notice to its contacts in the UK/EEA. A Data Privacy Impact Assessment (DPIA) and Legitimate Interest Assessment (LIA) confirmed that Lusha's processing activities align with legal requirements without infringing on individuals' rights.

4 Lusha's Privacy Practices

4.1 Certifications

Lusha's privacy practices and posture have been independently assessed by multiple third parties. Our attestations include:

4.1.1 **Accredited ISO 27701**: This certification provides a framework for holders of personally identifiable information to establish, implement, maintain, and improve a Privacy Information Management System (PIMS). Lusha has been audited for its data collection, B2B Data enrichment, verification, and prospecting services.

4.1.2 **ePrivacyseal EU**: The ePrivacyseal certification attests to a product's compliance with the GDPR. ePrivacy awards the GDPR seal of approval following an in-depth technical and legal audit of a company's digital products.

4.1.3 **TRUSTe CCPA Validation:** Lusha's privacy and data protection practices and governance efforts have been audited against TRUSTe's CCPA Privacy Practices Compliance Validation Requirements.

4.1.4 **TRUSTe Responsible AI Attestation:** Lusha's sales intelligence platform has been audited against TRUSTe's AI standards that cover compliance with the regulations of the EU AI Act, as well as principles from leading industry standards such as NIST and OECD guidelines.

4.1.5 **ISO 42001:** ensures that Lusha fill the requirements for establishing, implementing, maintaining, and continually improving a management system specifically designed to govern AI technologies safely and responsibly. I

4.1.6 **ISO 31700:** Concerning Privacy by Design, confirms that Lusha embeds customer privacy considerations in the lifecycle development of its products and services.

4.1.7 **ISO 27001**: Concerning Privacy Security, confirms that Lusha has been assessed and complies with the requirements of ISO 27001.

4.1.8 **ISO 27018**: Concerning Cloud Security, confirms that Lusha has been assessed and complies with the requirements of ISO 27018 Best Practices.

4.1.9 **SOC 2**: Ensures that Lusha safeguards customer data. The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.

To conclude, Lusha's security, AI, and privacy practices are audited annually by an impartial third-party auditor to ensure its highest standards.

4.2 Accountability

4.2.1 Data Accuracy: We have implemented internal mechanisms and proprietary algorithms to verify business profile information: each contact within our database must be verified by at least two separate, independent sources to be confirmed as a contact and entered into the database. This substantially mitigates the risk of incorrect or missing information within the database. Furthermore, our Business Contact Cards undergo regular review for validation and accuracy.

4.2.2 Data Minimization: Our core data set consists of categories of data that are strictly required to provide the services and are limited to basic business profile information that would typically be found on an email signature or business card. We do not include sensitive data in our B2B Database (such as identity numbers and biometric data).

4.2.3 Fair and Lawful Processing: via an annually reviewed DPIA we ensure that our data processing meets the requirements to enable lawful processing. The specific legal bases for processing are set out in our Privacy Policy, but in short, we contend that Lusha's processing of business profile information satisfies the "legitimate interest" basis for lawful processing, as described in detail under section 3.4 hereto.

4.2.4 Transparency: We are transparent about the data we process when we collect and afterwards. where required by law, we have processes in place to inform the relevant data subjects (by way of notice via email or SMS, as applicable) that Lusha holds their personal information. An example of this notice can be found here. This notice provides the data subject with all relevant information in accordance relevant regulation (e.g. Article 14 of the GDPR), including informing the data subject of their right to opt out before adding their data to Lusha's database and to exercise their other rights as required by law. Further, we have a dedicated online Privacy Center that provides data subjects with relevant and useful information about their data.

4.2.5 Individual Rights: We honor requests from individuals to opt out of our B2B Database, and we maintain a suppression list to ensure these rights are met. We also have processes in place to enable compliance with data subject rights on subject access, rectification, erasure, and restriction of processing. Lusha honors requests from data subjects to exercise their rights and provides a 24/7.

To conclude, Lusha is responsible for adhering to all privacy principles. Its accountability is assured via its policies, practices, and third-party annual audits,

4.3 Security

We implement the following robust security measures:

4.3.1 Encryption: Encrypted data storage solutions so that any personal data processed by Lusha is encrypted whilst in transmission, consistent with industry standards and at a minimum of 256-bit encryption.

4.3.2 Security policies and procedures: Security policies and procedures, including internal security audits, penetration tests, and implementation of security awareness training regarding the handling and securing of personal data to ensure employees and contractors process personal data to a standard aligned with leading data protection laws.

4.3.3 Security standards: To keep personal data safe and secure, such as state-of-the-art encryption (as described above), virus protection, firewalls, and intrusion prevention technologies to prevent any unauthorized access or compromise of Lusha's network, systems, servers, and applications from unauthorized access. Our security standards are audited by third parties and have been certified as meeting the ISO 27001, ISO 27018, SOC2 and CSA STAR standards (as described above).

4.3.4 Access controls: Access controls to ensure there are limits on access to information systems and facilities to provide reasonable assurance that access to data centers is limited to authorized individuals, such as coded badge access (physical controls), user authentication (logical controls), periodic reviews of changes affecting systems' handling authentication, authorization and auditing as well as privileged access to production systems and ensuring that any terminated employee's access to personal data will be immediately revoked.

4.3.5 Disaster recovery Involves a formal disaster recovery plan and incident response plans, regular testing of the effectiveness of the plans, and the implementation of backup controls such as periodic backups of production file systems and databases according to a defined schedule and a formal disaster to ensure business continuity and minimize the effects of unplanned events.

4.3.6 Internal policies: Policies and procedures for managing changes to production systems, applications, and databases, including processes for documenting, testing, and approving changes to production, security patching, and authentication.

Lusha safeguards personal data through a certified, enterprise-grade security framework that combines 256-bit encryption, strict physical and logical access controls, proactive disaster recovery planning, and rigorous third-party audits, including SOC2 and ISO 27001.

5 Customers' Responsibility for Marketing Activities

5.1 Privacy aspects: Customers are independent controllers.

5.1.1 Since Lusha and each of its customers have an independent controller–independent controller relationship with respect to the flow of data from Lusha to the customer, we would like to emphasize that both Lusha and each of our customers has the responsibility to ensure lawful data processing. Other than for outlining legal and contractually agreed-upon purposes and certain restrictions that apply with respect to the Platform and data usage, Lusha will not instruct you how to process your data.

5.1.2 If you enrich your data via the Lusha platform, you are deemed as already having a legal basis to process the data purchased from Lusha, since the data enrichment process involves sharing with Lusha personal data of business contacts that you have, in order for Lusha to enrich, cleanse and/or update such personal data against the data maintained in Lusha's B2B Database.

5.2 Our Features help you be compliant

Lusha has implemented a variety of features so customer can conduct their sales, marketing, and recruitment in a compliant way

5.2.1 Suppression list: Once a data subject opts out of Lusha's processing of their personal data, Lusha add such information to a suppression list, in order to prevent the inclusion of such data subject's data on the Lusha Platform, in the future.

5.2.2 Opt-out notice: When a data subject opts out of Lusha's database, Lusha notifies customers who have purchased information about the data subject that the data subject has requested to be removed. Customers are thereafter required to remove such data subject's contact details as acquired using the Lusha Platform unless the customer has an alternate lawful ground for retaining such information.

5.2.3 Hide contacts from specific jurisdictions: This feature allows customers to manage their account access to any country as desired, including imposing restrictions for certain jurisdictions. For enterprise customers who would like to avoid specific regulations covering marketing or other risks, our platform can be set to hide the information on a country-by-country basis.

5.2.4 Do-not-call: Lusha is an official cleaner of the TPS and CTPS in the UK and the DNC in the US. Admin of an account can choose to hide phone numbers purchased from Lusha listed on these Do Not Call lists and other DNCs, as available at the time.

Please note that currently, Lusha does not scrub data from other data vendors purchased via the waterfall service.

5.3 Customer best practices

5.3.1 Prior to accessing data from Lusha's B2B Database, customers must be aware of the applicable legislative and regulatory landscape regarding direct marketing practices in the jurisdiction(s) in which they intend to use the data for their activities that fall under one of the permitted purposes.

5.3.2 Lusha complies with privacy laws applicable to it – but customers need to, as well. Each country has its own direct marketing requirements (not to spam, harass, etc.), and certain uses have their own specific requirements as well. Subject to compliance with those laws, our platform can be used for sales, recruiting, marketing, and fraud prevention.

5.3.3 We have created an interactive privacy map to help you determine which laws and requirements may apply to your direct marketing activities. It is the customer's responsibility to analyze its proposed use cases for the data obtained from Lusha's platform and to identify how it can use it in a compliant manner.

5.3.4 The biggest myth about the GDPR is that consent is the ONLY way to lawfully process personal information on EU data subjects. While consent is one lawful basis for processing, it is not the only one. Most of our customers will process the personal data on a "legitimate interest" basis, which includes direct marketing purposes. (See Id. Art. 6(1)(f), Recital (47).) In such a case, consent is not needed, but a transparency notice explaining your processing activities is required (See Id. Art. 14.). So, if you obtain a new list for email marketing, you could include the notice with your first message - however typically organizations send a standalone notice prior to engaging in any commercial activity.

5.3.5 In any case, since emailing a prospect is done only after a sales phone call, most of our customers may not even have a need for an Art. 14 notice since the conversation over the phone already created a legitimate expectation. Please note that B2B calling is exempt from Do Not Call Lists in many jurisdictions.

To conclude, Lusha's is responsible for all the privacy aspects of collecting and selling personal data to customers. Customers are responsible for their own use of the data (e.g., with respect to local privacy and marketing laws)

6 Additional information we want you to know

6.1 Use of customer data

Lusha requires certain customer information to provide its customers with access to the Lusha platform and to set up end-user accounts. Additionally, if you choose to connect your CRM, Lusha can provide you with enriched data and relevant insights. Any additional information that the customer shares with Lusha is at the customer's sole discretion and is provided by the customer on a voluntary basis.

Lusha does not sell customer data of paying customers; we only share it with those affiliates and service providers required to provide the service to the customer and to improve the service. Further, customer data is kept physically separate from the Business Contact Cards that form Lusha's database. Only if applicable, customer data may be transferred in connection with an asset sale, merger, bankruptcy, or other business transaction.

6.2 Post Termination

Unless the customer breaches our agreement, the Customer may retain the data purchased via Lusha forever without an obligation owed to Lusha to delete or return the data obtained from Lusha's B2B Database.

6.3 AI Usage

Lusha may make certain features available, including artificial intelligence ("**AI**"), machine learning, or similar functionality ("**AI Features**"). These features may include technology developed by Lusha or a third-party provider. In furtherance of our commitment to ethical AI practices, we have obtained a Responsible AI Certification from TRUSTe and ISO 42001 to ensure safe AI usage..

Lusha uses machine learning to provide better recommendations and make search results faster. We actively train our models with bias mitigation techniques and monitor output to reduce bias. We have implemented built-in controls to uphold data integrity while our additional guardrails catch formatting issues, reduce hallucinations, and ensure factual accuracy. Additionally, our AI tools undergo rigorous testing and evaluation.

Lusha acknowledges that customer data provided by the customer via its account's integrations and enrich services is confidential. Lusha is committed to safeguarding customer data and respecting its users' privacy. Therefore, Lusha confirms that it will not use customer data to train public AI. Notwithstanding, AI Features may be trained in Lusha's local and offline environment for product and research development purposes,

mainly with regard to customers' metadata. For example, AI Features may analyze what certain companies (in the same size and industry as the customer) are searching for in Lusha's Platform and recommend to other customers how to get better enrichment results based on such searches. Customers may elect to opt out of the use of its data to train Lusha's AI, however, please be advised that as a result, certain Lusha Platform functionalities (such as Lusha's Flex AI Suggestions and AI Recommendations), may be limited or impaired.

Please refer to our Privacy Center for further information.

If you have any questions about our privacy practices, please email us at: privacy@Lusha.com.

Sincerely,

Assaf Gilad (CIPP/US, CIPP/E), DPO

Annex A – GDPR

Lusha: GDPR

At Lusha, privacy is important to us. We are committed to data protection and transparency about our data practices. We have prepared this white paper so you can learn about the data we process, how we use it, and how we comply (and help our customers comply) with relevant privacy laws.

A key data protection law is the EU General Data Protection Regulation and the UK Data Protection Act 2018 (the "**UK GDPR**", and together with the "**EU GDPR**",, the "**GDPR**"). The GDPR requires organizations to develop robust data protection programs with an emphasis on accountability, transparency, individual rights, and security. Below, we address the measures Lusha has taken to comply with the GDPR. We do not address each provision of the GDPR but give a broad overview of how the GDPR relates to Lusha and the provision and use of its services.

We are dedicated to offering the best service to our customers, including assisting them in meeting their obligations under applicable data privacy laws. As evidence of our high level of data protection and privacy standards, we have been audited and found to be compliant with ISO 27701 and related GDPR requirements, ISO 27001, ISO 27018, and ISO 31700 (all such certifications and/or attestations are available on request). Obtaining ISO 27701 is a testament to our unmatched levels of data privacy and compliance in the B2B sales intelligence industry.

1. LUSHA'S ROLE IN DATA PROCESSING AND GDPR COMPLIANCE

1.1. Our customers make independent decisions about what personal data to collect and how and why data is processed. Under our interpretation of the principles of the GDPR, our customers are independent data controllers with respect to the data that they receive from us. Similarly, we make decisions about the personal data we process, including the information in our database. In this respect, Lusha acts as an independent data controller, and when the data from Lusha's database is transferred to a customer of Lusha, the customer becomes an independent controller of such data. As a result of the independent controller-independent controller relationship between Lusha and the customer, each party has its own independent obligations under GDPR and other applicable laws. We recommend that customers subject to the GDPR remain cognizant of their own obligations in respect thereto (in addition to potential obligations set out in applicable Marketing Laws (defined below) or otherwise).

1.2. In specific situations, and where a customer is subject to the GDPR, Lusha might be considered a data processor in respect of the processing of data specifically provided by

the customer to Lusha. This, for example, occurs when a customer sends Lusha the names and email addresses of their employees, which details are needed to set up accounts with Lusha and provision them as end-users on the customer's account. In this situation, Lusha acts solely on our customer's instructions.

1.3. Lusha is committed to complying with all laws and regulations to which it is subject, and assisting our customers in meeting their compliance obligations.

2. HOW LUSHA HELPS CUSTOMERS COMPLY WITH THE GDPR

2.1. To help our customers comply with the GDPR, we have implemented the following:

2.1.1. **Data processing agreements (DPAs**): We have robust data processing agreements in place with our customers that meet the contractual requirements set forth in Article 28 of the GDPR, which can be reviewed here. In respect hereof, we only process personal data provided to us by customers on the instructions of the information-providing customer (as set out in the DPA).

2.1.2. **Sub-processor diligence**: A thorough due diligence and security and privacy review is undertaken in respect of vendors who might process any customer personal data. We have procedures in place to ensure that these vendors will not gain access to customer personal data unless they have entered into data processing agreements that meet the Article 28 requirements for compliance with EU/UK laws.

2.1.3. **Data transfers**: There are certain restrictions on the transfer of data outside of the EU and UK imposed by the GDPR. To ensure the continued protection of the data, any personal data that is transferred is subject to appropriate safeguards. Once we receive customers' information, we take all appropriate technical and organizational measures and reasonable precautions and follow industry best practices to safeguard such information against loss, theft, unauthorized use, access, or modification. Where applicable, e.g., when our customers are subject to the GDPR and export data to us, we have signed contracts based on the Standard Contractual Clauses approved by the European Commission or similar contracts, ensuring essentially the same level of protection for further transfers.

2.2. **Security**: We implement the following robust security measures:

2.2.1. **Encryption**: Encrypted data storage solutions, so that any personal data processed by Lusha is encrypted whilst in transmission, consistent with industry standards and at a minimum of 256-bit encryption.

2.2.2. **Security policies and procedures**: Security policies and procedures, including internal security audits, penetration tests, and implementation of security awareness training

regarding the handling and securing of personal data to ensure employees and contractors process personal data to a standard aligned with leading data protection laws.

2.2.3. **Security standards**: Security standards to keep personal data safe and secure, such as state-of-the-art encryption (as described above), virus protection, firewalls, and intrusion prevention technologies to prevent any unauthorized access or compromise of Lusha's network, systems, servers, and applications from unauthorized access. Our security standards are audited by third parties and have been certified as meeting the ISO 27701, ISO 27001, ISO 27018 and ISO 31700 standards (as explained above).

2.2.4. **Access controls**: Access controls to ensure there are limits on access to information systems and facilities in order to provide reasonable assurance that access to data centers is limited to authorized individuals, such as coded badge access (physical controls), user authentication (logical controls), periodic reviews of changes affecting systems' handling authentication, authorization and auditing as well as privileged access to production systems and ensuring that any terminated employee's access to personal data will be immediately revoked.

2.2.5. **Disaster recovery:** Formal disaster recovery and incident response plans, regular testing on the effectiveness thereof, and the implementation of backup controls such as periodic backups of production file systems and databases according to a defined schedule and a formal disaster to ensure business continuity and minimize effects of unplanned events.

2.2.6. **Internal policies**: Policies and procedures for managing changes to production systems, applications, and databases including processes for documenting testing and approval of changes into production, security patching, and authentication.

3. LUSHA'S PRIVACY COMPLIANCE STRATEGY

3.1. We take a serious approach to privacy compliance, and set out our main measures below:

3.1.1. **Accountability**: We take an accountable, privacy-first approach, and in particular, focus on the following:

3.1.1.1. **Data Accuracy**: We are committed to data accuracy. We have implemented an internal mechanism to verify business profile information: each contact within our database must be verified by at least two separate, independent sources to be confirmed as a contact and entered into the database. This substantially mitigates the risk of incorrect or missing information within the database

3.1.1.2. **Data Minimization**: We follow data minimization principles. Our core data set consists of categories of data that are strictly required for the purpose of providing the services

and is limited to basic business profile information (that would typically be found on an email signature or business card).

3.1.1.3. **Fair and Lawful Processing**: We ensure that our data processing is fair and lawful, meeting the requirements to lawfully enable the processing. The specific legal bases for processing are set out in our Privacy Policy, but in general, we assess that Lusha's processing of business profile information satisfies the "legitimate interest" basis for lawful processing, with the specific legitimate interest to enable businesses to achieve commercial success through accessing limited professional and business information of individuals [including those in the EU/UK who have not opted out when given the opportunity to do so]. To the extent there is a concern that the individual would not reasonably expect further processing, each individual has the right to be removed from our database upon request – see more on individual rights below.

3.1.2. **Transparency**: We are transparent about the data we process. When we collect business contact information about individuals, where required by law in the EU/UK, we have processes in place to inform the relevant data subjects (by email or SMS, as applicable) that Lusha holds their personal information. This notice provides the data subject with all relevant information as required by Article 14 of the GDPR, including informing the data subject of their right to opt-out. We strive to provide individuals with an easy way to exercise their transparency rights including being able to obtain information about the purposes for which their data is being used, and the categories of recipients to whom their data is disclosed (i.e. our customers who license the data for their B2B sales and marketing purposes). Please refer to our Privacy Policy for further details.

3.1.3. **Individual Rights**: Individuals – both in our database and customer end-users – can exercise their rights at any time. For example, we honor requests from individuals to opt out of our database, and we maintain a suppression list to ensure the rights are met. We also have processes in place to enable compliance with data subject rights on subject access, rectification, erasure, restriction of processing, and data portability. Lusha honors requests from data subjects to exercise their rights (most commonly, the right to be removed from our database).

3.1.4. **Security**: For more information about our security program, see above.

3.2. By default, during our engagement with our customers, any personal data that we collect from our subscribed customers in our capacity as processor role is not included in our B2B database unless agreed otherwise.

3.3. Following the Schrems II decision, Lusha withdrew from the Privacy Shield program and currently only allows for international data transfer based on an executed data processing agreement, which maintains the confidentiality of your data and incorporates data protection obligations consistent with applicable privacy laws. For a full list of sub-processors visit (and subscribe to updates thereof) our sub-processors page.

4. GDPR APPLICABILITY

4.1. Although we align our data protection practices with the GDPR principles and are determined to be compliant therewith, as indicated by our ISO 27701 certification, and ePrivacy Seal, Lusha was found in November 2022 by the French data protection authority that the GDPR does not apply to Lusha directly regarding the data we provide to our customers for the following reasons:

4.1.1. Lusha is incorporated in the United States, with no 'establishments' in the EU/UK, and therefore does not fall within the territorial scope of the GDPR in respect of the GDPR's establishment criterion.

4.1.2. Lusha does not directly offer its products or services to individuals based in the EU/UK. For example, we do not accept payment for our services in local currency, run local-EU/UK domains for the services or provide the service in an EU/UK language other than English. We only offer our products on a B2B basis, and therefore do not fall within the scope of the GDPR in respect of the offering criterion.

4.1.3. Finally, Lusha does not monitor individuals in the EU/UK, nor does it make decisions or predict preferences and attitudes of such individuals. Lusha does not monitor the contacts in its database within the meaning of the GDPR and therefore does not fall within the territorial scope of the GDPR in respect of the monitoring criterion

4.2. On July 2026, the Italian Data Protection Authority – Garante – published a decision finding Lusha's 2025 practices to be non-compliant with certain provisions of the GDPR. We disagree with the Garante's findings and will appeal the decision, as permitted under applicable law and regulation.

4.3. Most of the issues upon which the Garante based its decision have since been remediated. Moreover, the Garante's finding that Lusha did not have a legitimate interest in collecting and providing certain business contact data to customers is one we fundamentally disagree with, and we remain confident that the way we process data for our customers is fully aligned with the GDPR.

4.4. We recognize that data protection and compliance are at the core of our business and the relationships we maintain with our customers and partners. This is not a responsibility we take lightly, and we invest significant time and resources to ensure our alignment not only with the GDPR but with any applicable data protection laws and principles.

4.5. Lusha has long maintained a robust privacy and compliance program that includes GDPR alignment at its core. This includes compliance with the highest global privacy and security standards, and we maintain ISO 27701, ISO 27001, ISO 27018, and SOC 2 Type 2 certifications. We have also conducted independent, third-party audits and certifications to ensure our consistent alignment with GDPR.

4.6. GDPR alignment is built into Lusha's DNA, both from a product and personnel perspective. Our product development cycle includes controls, processes and policies that ensure continued GDPR alignment, and we maintain a global privacy training program that our employees are required to complete on an annual basis.

4.7. As we have said, we will appeal this decision and look forward to the opportunity to demonstrate our continued commitment to privacy compliance.

.

5. USE OF OUR DATA

5.1. We would further like to highlight the different legal roles held by Lusha and each of our customers. While it is incumbent upon Lusha to comply with relevant and applicable privacy laws (such as GDPR), if our customers use the data obtained from Lusha for marketing purposes, they must comply with applicable electronic communication and/or direct marketing laws ("**Marketing Laws**"), which laws are in place to regulate same. The specific Marketing Law(s) with which customers must comply depend on the location of the customer, the location of the data subject receiving the marketing material, and the requirements in respect thereto vary from jurisdiction to jurisdiction. We strongly recommend that customers obtain legal advice on how best to comply with relevant Marketing Laws because the requirements/exemptions for use of data for B2B communications differ.

5.2. If you have any questions about our privacy practices, please email us at: privacy@Lusha.com.

Annex B – GDPR ePrivacy Seal

CERTIFICATE

no. 535/26

ePrivacyseal GmbH
Bei den Mühren 5, 20457 Hamburg, Germany

hereby certifies* that

as determined in the certification decision of 28 July 2026

Lusha Systems Ltd
132 Derech Menachem Begin, Tel Aviv 6701101, Israel
as a controller in the sense of art. 4(7) GDPR

operates its product or service
"Lusha's Prospecting Platform" and "Integrations solution"
version as available February 2026
as defined in annex 1 and to the exclusion of the processing activities in annex 2 to this certificate.

final audit day: 28/07/2026
next planned monitoring by 19/01/2029
period of validity: 20/02/206 – 19/01/2029

The certification decision takes place under the validity condition described in Annex 3
and in conformity with the criteria catalogue for the "ePrivacyseal EU" (version 3.0 of May 2022)
of ePrivacyseal GmbH.

Annex C – CCPA/CPRA

Lusha: CCPA/CPRA

This annex summarises our interpretation of the CCPA/CPRA as it applies to Lusha's product and its use thereof by our customers. Data subjects (as defined in the GDPR) are referred to herein as 'consumers.'

Lusha is a registered data broker in the State of California.

Pursuant to Section 999.305(d) of the regulations issued by the California Attorney General in October 2019, a business that does not collect its data directly from the consumer is not required to provide the "pre-collection" notice. However, such businesses are required to notify the consumer directly prior to selling that consumer's information. The notice must state that the business sells information about the consumer and notify the consumer of their right to opt-out.

In order to comply with this requirement, Lusha has provided, and will continue to provide, direct notifications to all California-based contacts in its database. Further, Lusha has an automated process for providing notifications to any new California-based contacts as they are added over time. We have also expanded the notification process to cover our entire database so that we are providing notices regardless of the consumer's location.

In addition to the direct, pre-sale notification requirement, the CCPA requires businesses to disclose certain information to consumers regarding the collection and processing of personal information, as well as describe certain consumer rights, such as the right to opt-out. These disclosures are included in Lusha's privacy notice, available at https://www.lusha.com/legal/privacy_notice/.

Consumer Rights

In addition to the notice and disclosure requirements, the CCPA grants California consumers the right to know what information a business has about them, to opt-out of the sale of information, and to have their information deleted. Lusha maintains a dedicated Privacy Center where individuals may exercise their rights accessible at https://www.lusha.com/privacy-center/. Further, they may select the "Do Not Sell My Info" button on our homepage. From within the Privacy Center, a consumer can submit a request to access the information we have about them or submit a deletion or opt-out request. Consumers can also claim their profile, which allows them to not only view their information but make changes if they wish. Access, opt-out, and deletion requests are handled by our

dedicated privacy team and typically processed within 7 business day, far less than the 45 days allotted under the regulations.

Use of Lusha Data and Other Personal Information

Pursuant to Section 999.305(d), because our customers are obtaining this information from us and are not selling it, they do not need to provide active notifications to the contacts obtained from Lusha. If our customers are subject to the CCPA, however, they will need to honor consumer requests to access and delete their data from your possession, in addition to the other compliance protocols undertaken in respect of the CCPA, such as updating privacy notices.

Annex D – CCPA Validation Letter

TRUSTe CCPA Validation Findings Summary[1]

Expiration date: August 3, 2027

Scope

TRUSTe, the Assurance division of TrustArc, Inc. have reviewed practices that govern the Privacy Program of Lusha Systems Ltd. ("Organization") as of August 3, 2026 against the CCPA Controls ("Controls"). These Controls are based on the mapping of the CCPA, to the TrustArc Privacy & Data Governance ("P&DG") Framework. The Controls focus on measures for demonstrating that the processing of personal information conducted by Lusha Systems Ltd. is performed at a control effectiveness level consistent with the Controls. The Controls cover the following areas aligned with the **BUILD**, **IMPLEMENT** and **DEMONSTRATE** Standards set forth in the TrustArc Privacy & Data Governance ("P&DG") Framework, for establishing, maintaining, and continually improving adherent data protection practices.

Inherent Limitations

Because of their nature and inherent limitations, practices-level measures of the Organization may not always operate effectively to meet the applicable Controls. Furthermore, our findings herein are subject to the risk that the Privacy Practices, or any component of the Organization's practices, may change or that practice-level measures implemented by the Organization may become ineffective or fail.

Findings

In our opinion, in all material respects, based on the representations made by relevant personnel and supporting evidence of practices-level measures identified in Lusha Systems Ltd.'s CCPA Validation Assessment:

- The applicable practices-level measures as further described in the accompanying CCPA Validation Report have been implemented as of August 3, 2026.
- The measures described in the CCPA Validation Assessment were suitably designed to provide reasonable assurance that the Controls would be met if the practices-level measures operated effectively as of August 3, 2026

Restricted Use

This summary of the Findings Letter and accompanying report is for the intended use of Lusha Systems Ltd. as of August 3, 2026.

- This summary provided by TRUSTe may be used by the Organization until its expiration date listed below.
- This summary expires on August 3, 2027.

It is not intended to be, and should not be used nor relied upon by anyone other than the Organization and, as determined in the sole discretion of the Organization, the Organization's customers, contractors and other permitted stakeholders.

[1] This summary is solely an abbreviated unofficial version of the full Findings Letter and accompanying report. It is intended solely for the Organization to display on its website. No modifications to this document are permitted and shall render it invalid. Only the full Findings Letter and report represent the official determination of TRUSTe.

Annex E – ISO 27701

RONET International Certification Services Ltd.

Certifies that Privacy Information Security management system of:

Lusha Systems Ltd

132 Menachem Begin st.
Tel Aviv. Israel

Has been assessed and registered as meeting the International standard requirements of:

ISO 27701:2019

standard within the scope of activities detailed below:

Privacy Information Management System in development, sales and support of Lusha platform

Within the above certification scope, the role of the organization is: Processor and Controller

The version of the SoA including ISO 27001 and ISO 27701 controls is: 16 January 2025

The organization fulfills both ISO 27001 and ISO 27701 controls

Effective From: 27 February 2025 Valid Until: 04 April 2027

Original Approval Date:04 April 2024 Certification No.: P5902

Ronen Tuchfeld C.E.O

This certificate remains valid subject to satisfactory Surveillance visits conducted by RONET I.C.S. Ltd.
With accordance to the agreement and code of practice.
Main office: Maor 27, M.P. Hefer 38830, IL
www.ronet-ics.com

ANAB ACCREDITED MANAGEMENT SYSTEMS CERTIFICATION BODY

RONET International Certification Services Ltd.

Annex F – ISO 31700

RONET International Certification Services Ltd.
Certifies that Information Security for Cloud Services management system of:

Lusha Systems Ltd

132 Menachem Begin St.
Tel Aviv, Israel

Has been assessed and registered as meeting the International standard requirements of:

ISO 31700-1:2023

standard within the scope of activities detailed below:

Privacy by design within development, sales and support of Lusha platform

The integrated SoA version for ISO 27001 controls and ISO 27017 controls is 16 January 2025

ISO 27701 certificate no. IS902 valid until 04 April 2027

The organization fullfils both ISO 27001 and ISO 27701 controls

Effective From: 07 July 2024 Valid Until: 04 April 2027

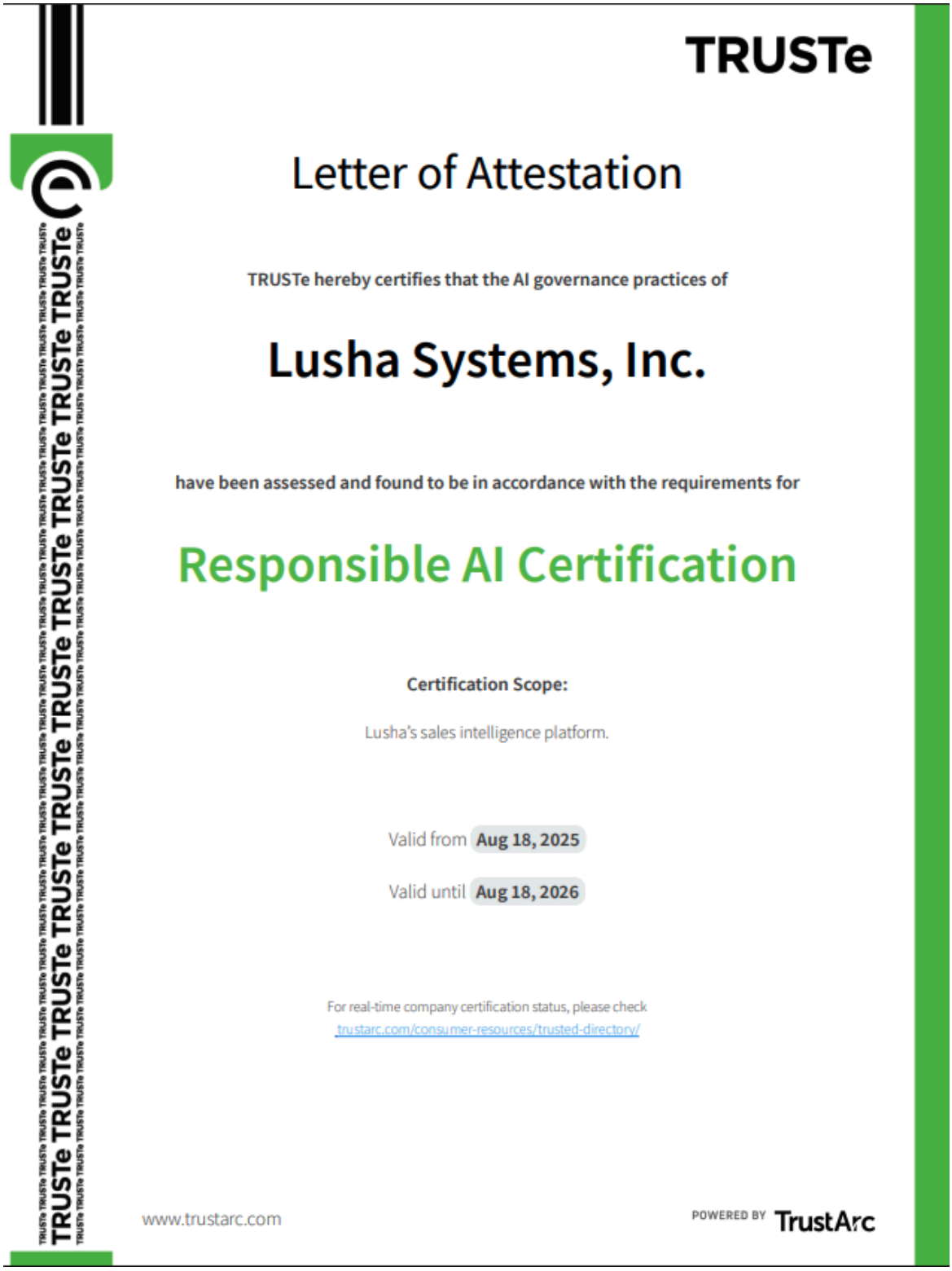
Original Approval Date: 07 July 2024 Certification No.: 5902

Ronen Tuchfeld C.E.O

This certificate remains valid subject to satisfactory Surveillance visits conducted by RONET I.C.S. Ltd.
With accordance to the agreement and code of practice.
Main office: Maor 27, M.P. Hefer 38830, IL
www.ronet-ics.com

RONET
International Certification Services Ltd.

Annex G – TRUSTe AI Certification



TRUSTe

Letter of Attestation

TRUSTe hereby certifies that the AI governance practices of

Lusha Systems, Inc.

have been assessed and found to be in accordance with the requirements for

Responsible AI Certification

Certification Scope:

Lusha's sales intelligence platform.

Valid from **Aug 18, 2025**

Valid until **Aug 18, 2026**

For real-time company certification status, please check
trustarc.com/consumer-resources/trusted-directory/

www.trustarc.com

POWERED BY TrustArc

TRUSTe TRUSTe TRUSTe TRUSTe TRUSTe TRUSTe TRUSTe TRUSTe

Annex H – ISO 42001 AI Certification

RONET International Certification Services Ltd.

Certifies that Information Security in Artificial intelligence management system of:

Lusha systems ltd

132 Menachem Begin st.
Tel Aviv, Israel

Has been assessed and registered as meeting the International standard requirements of:

ISO 42001:2023

standard within the scope of activities detailed below:

Development, sales and support of Lusha platform

Effective From: 18 May 2026 Valid Until: 18 May 2029

Original Approval Date: 18 May 2026 Certification No.: AI5902

Ronen Tuchfeld C.E.O

This certificate remains valid subject to satisfactory Surveillance visits conducted by RONET I.C.S. Ltd.
With accordance to the agreement and code of practice.
Main office: Maor 27, M.P. Hefer 38830, IL
www.ronet-ics.com

RONET
International Certification Services Ltd.