Interlynx Systems - Privacy Policy

Effective Date: May 2018 Updated: Dec 2020

'INTERLYNX; 'we'; 'us'; and 'our'; means INTERLYNX Systems LLC, Rincon, Puerto Rico USA.

We are committed to maintaining the highest standards of compliance with regulatory environments such as the EU General Data Protection Regulation (EU GDPR), UK General Data Protection Regulation (UK GDPR) and the California Consumer Privacy Act (CCPA). This Privacy Policy aims to explain to the Users of our Systems and Products ("Clients") how we process your personal data, so that you can make well-informed decisions regarding your information.

We may update this Privacy Policy from time to time to keep up with legislative or regulatory changes, and to ensure that it remains in-line with our business needs and obligations. Any update or modification of the current version of this Policy will be considered applicable from the time of its publication.

By using our Systems or Products, you are presumed to have read and understood this Privacy Statement.

When does this Privacy Policy apply?

This Privacy Policy will apply to personal information collected through the use of our Services and Systems. This policy applies to the personal information that we collect, use or ask you to provide to help us deliver our Services to you, as our client. When you subscribe to the systems offered by us or contact our team by email/phone, we are the Controller of the data being processed.

Data that we collect

The privacy and security of your information is of utmost importance to us. In the course of using our Services, we may come into possession and process personal information to fulfil our contractual obligations with you as a client or customer. Depending on your relationship with us, this information may include:

- Client Contact Data – business contact name, company name, company mailing address, email address, phone number, LinkedIn Profile URL
- Lead Contact Data – type of lead, date of lead, contact name, contact or job title, company name, mailing address, county, website URL, phone number supplied, phone number researched, parent company name, SIC, SIC Description, NAICS, NAICS Description, Line of Business, Source of Lead
- Sales Data – Sales and financial information, feedback from distributors and users
- Customer Support Data - Information you provide to us during customer service interactions and to receive technical assistance from us
- Connection Data – Server address, web browser type and settings, domain names, device type, IP address, Operating System (if applicable), Internet Connection type
- Performance Data – information on the performance of our systems
- System data – Aggregated data or other information that does not identify individuals.

- Statistical data: Data that is anonymised to obscure identification.
- Marketing Data – Marketing preferences (opted in/out status)

How we use the data we collect

For data that is supplied as part of our Services, we may use the data you provide to us to:

- Performance of a contract – Clients - Create and manage your account and system(s) functionality and troubleshoot any performance errors.
- Performance of a contract - System Users - Send sales lead reports and notification to clients, distributors, reps and customers related to feedback requests, reports and other support communication about our services and how it is used.
- Performance of a contract – Lead Generation – to research and propose missing information from existing sales leads to formulate a full customer lead

  Please note that if you are a client or user do not wish to be contacted for marketing purposes, you can inform our organisation, either by unsubscribing or informing us of your request to object to processing.

What grounds do we process your data under?

As above, you will see references to the [lawful basis] we use to process your data. The EU and UK GDPR forbids the processing of personal data unless it is in line with one of 6 lawful bases. The lawful bases we rely on are:

- Consent: when an individual has given clear consent for their personal data to be processed for a specific purpose. This consent must be well-informed and freely given.
- Performance of a Contract: the processing is necessary for a performance of a contract, or because they have been asked to take specific steps before entering into a contract.
- Legal Obligation: the processing is necessary for us to comply with the law (not including contractual obligations)
- Vital Interests: the processing is necessary to protect someone's life.
- Public Task: the processing is necessary to perform a task in the public interest or your official functions, and the task or function has a clear basis in law.
- Legitimate Interests: the processing is necessary for legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests <This cannot apply if you are a public authority processing data to perform official tasks>

If we are relying on consent for specific processing, you will always be offered the opportunity to withdraw your consent at any time. However, if you would like to object to direct marketing, you can do this regardless of the lawful basis we rely on. You can unsubscribe using the unsubscribe link at the footer of any marketing material you receive from us, or by e-mailing us directly at info@INTERLYNXsystems.com We aim to action your action as soon as reasonably practicable.

How long do we keep your personal data?

We process personal data only for as long as necessary to achieve the purposes for which it was originally collected. After that purpose has ended, we will securely expunge your data without undue delay. We monitor this to ensure this is carried out within the relevant timescales, as part of our accountability obligations.

We will also retain your Personal Data as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Security of your data

The security of all personally identifiable information associated with our clients, users and systems is of paramount consideration to us. Because of the open-forum nature of the internet, it is not possible for us to guarantee the safety of data.

INTERLYNX has implemented technical and organisational security measures to limit the risk of loss, misuse, wrongful disclosure or alteration of personal data. Please be assured that we are constantly reviewing our security procedures, including high levels of security encryption. Our measures include:

- Secure servers latest security technology
- We provide secure domains to our clients
- OTP authentication techniques
- Secure FTPs (File Transfer Protocol) for data transfer
- Data disclosure for strictly necessary INTERLYNX personnel only
- Regular expunging of sensitive data not required to fulfil our contractual obligations
- INTERLYNX ensures all personnel undertake awareness programs and training on how to handle client data securely
- INTERLYNX has also implemented a Disaster Recovery Plan which can be utilised in the event of major business disruption (i.e., due to COVID-19, Attacks, Unrest etc)

Who do we share your data with?

Data that is not essential to the services we provide to our clients is expunged immediately. INTERLYNX does not share your data with anyone else, except where:

- INTERLYNX are required to do so by law or in the good-faith belief that such disclose is reasonably necessary to respond to subpoenas, court orders, or other legal process.
- Technology service providers who host our information systems, back up servers or that offer us technological support and integrations, such as HubSpot, Salesforce, Tour de Force, Microsoft Dynamic CRM, ZOHO, Prophet 21 and NetSuite
- Our legal advisors when a claim is presented in relation to our services and products.
- In the event that we sell or buy any business or assets, in which case we may need to disclose your data to the prospective seller or buyer, or new business partner

Processing data of UK ("UK GDPR") or EU Citizens ("EU GDPR"):

Both the EU and UK GDPR are regulations that require businesses to protect the personal data and privacy of EU and UK citizens for transactions that occur within EU member states. GDPR promotes the secure and honest processing of personal data, which is information that can lead to the identification of an individual. For more information on both UK and EU GDPR, please visit the Information Commissioner Office's website (www.ico.org.uk). The ICO are the UK regulator for data protection.

We are committed to ensuring transparency in our processing. We are open and honest about the data that we collect and what we do with it. We will only ever use the data we collect for the purpose we first acquired it, and always in a manner that you would expect. We will only collect the necessary type and amount of data we need to achieve the purpose and will retain it for as little time as possible.

GDPR imposes a number of principles onto organisations who process data. These are as follows:

- Principle A – lawfulness, fairness and transparency of processing
- Principle B – purpose limitation (only use data for the original purpose it was collected)
- Principle C – data minimisation (data collected must be adequate, relevant to the purpose and limited to what is necessary to achieve the purpose.
- Principle D – Accuracy (data collected must be kept up-to-date and accurate)
- Principle E - Storage Limitation (data must only be retained for the necessary amount of time)
- Principle F – Integrity and Confidentiality (have appropriate measures in place to ensure security of data)

Whenever we transfer the personal data of an EU/EEA individual out of Europe, we ensure a similar degree of protection is afforded to it as it would be intra-EEA by ensuring at least one of the following safeguards are present:

- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection as it has in Europe called Standard Contractual Clauses (SCCs)
- Please note that following the Court of Justice of the European Union ("CJEU") on 12 July 2020, Data Transfers between EU and US can no longer rely on the Privacy Shield scheme as an appropriate safeguard.
- From 31 December 2020, the United Kingdom will no longer be a part of the EU/EEA. INTERLYNX will also comply with the UK GDPR.

California Consumer Privacy Act ("CCPA")

The California Consumer Privacy Act (CCPA) gives consumers more control over the personal information that businesses collect about them.

This law secured new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared.
- The right to delete personal information collected from them (except data retained by law)
- The right to opt-out of the sale (disclosure) of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.
- To require INTERLYNX to respond to verifiable requests with disclosures about the personal information that we collect, sell or disclose;

INTERLYNX ensures that the data we receive via any means is secure and protected. Please see 'Data Security' below for more information. You can exercise any of your rights under CCPA by contacting us at info@interlynxsystems.com

Processing the data of minors under 13 years

We do not direct any features in our Products to children under the age of 13. Children under 13 may not register with INTERLYNX, including downloading, installing or using any of the systems available. Whilst INTERLYNX systems do not currently apply to children, any forthcoming system versions intended for use by children will always require parental or guardian consent, in line with Children's Online Privacy Protection Act ("COPPA") rules.

Any such system versions will also provide parents with access to information collected about their child and the opportunity to opt-out of future processing and have us delete such information at any time. INTERLYNX strongly encourages parents and guardians to supervise their children's online activities and to consider using parental control tools available from online services and software manufacturers to help provide a child-friendly online environment. These tools also can prevent children from disclosing online their name, address, and other personally identifiable information without parental permission. Products and services for sale are intended for purchase by adults. By making a purchase on the Website, you agree that you are at least 13 years of age.

In line with COPPA regulations, INTERLYNX and our Products will...

- Never collect personally identifiable off-line contact information from children under the age of 13 without prior parental consent.
- Never distribute to third parties any personally identifiable information with respect to children under the age of 13 without prior parental consent.
- Never give the ability to post publicly or otherwise distribute personally identifiable contact information with respect to children under the age of 13 without prior parental consent.
- Never entice children under the age of 13 by the prospect of a special game, prize or other activity, to divulge more information than is needed to participate in the activity.

Marketing

You can unsubscribe from marketing communications from us at any time. You can use the unsubscribe link at the footer of any marketing correspondence we have sent you, or by contacting us directly asking us to unsubscribe you by emailing info@INTERLYNXsystems.com

Links to other sites

This Privacy Policy does not apply to any third-party links provided to you by us. Third parties will appoint their own privacy policies, and these should be consulted should you have any queries about how they process your data. We have no control over such third-party processing and are not responsible for their actions.

Contact Details

If you have any concerns regarding our processing of your data, we would appreciate the opportunity to resolve this directly with you. Please contact us by:

- By email: info@INTERLYNXsystems.com or by;
- By mail: U.S. Mail at INTERLYNX Systems, LLC, PO Box 127, Rincon, Puerto Rico 00677.

If we cannot resolve your concern to your satisfaction, you have the right to complain the data protection regulator for your country.