Our GDPR policy

This is a copy of our GDPR policy which sets out how we use and protect personal information. It sets out the information that we collect and hold.

We may collect and process the following personal information about customers:

Contact

Your name, business address, how to contact you. We use this for servicing your evaluation of or use of purchased products and services, marketing, enhancing our products and services offerings.

Transactional

Bank and/or credit card details, how you use our products and services, changes you make to your product(s) or account. We use this for servicing your account and for making changes as required by you on the data that we hold.

Contractual

Your purchase and payment history and creditworthiness.

Technical

Details of the devices and technology that you use. We use this for administering the authorization to use licensed applications.

Open Data and public records

We may collect information about you that is provided by credit card processors, as well as that made generally available by publication on the Internet or from other public sources such as company registries. We use this for account administration purposes.

Where do we obtain information?

Principally from information you give us directly when you fill in forms or contact us directly by telephone or other means for the purposes of contracting for services or carrying out product evaluations. Information that we collect about you or receive from other sources includes reports from credit card agencies, from Internet searches including searching ‘social media.’

How do we use your information?

Principally to carry out our responsibilities resulting from the agreements that have been entered into – the evaluation of or license purchase for our products and services, and to provide you with information, products and services that you have requested. This includes marketing information about changes to existing products, including end-of-life advice and services as well as new systems. We also use your information to comply with applicable legal or regulatory requirements, including limitations on the export of dual-use encryption technologies.
Using your information in accordance with Data Protection Regulations

Data protection regulations require us to meet certain conditions before we’re allowed to use your personal data in the way that we describe in this policy document. We take these responsibilities very seriously, and rely upon the following conditions or reasons, depending on the activities we are carrying out. Each of the reasons is now explained in more detail.

Contractual reasons

Providing contracts and services to a customer. When evaluations are requested they are granted in the expectation of forming contract to supply and communications to the collateral actions of administering the evaluation are reasonable, provided they are to do with the conduct of the evaluation, and not merely marketing materials. It is legitimate to contact existing and potential customers concerning the conduct of their accounts, to chase quotations and invoices, to respond to customer service requests and to follow up any of these actions in furtherance of the operational requirements of both parties. This includes following up evaluation accounts (which are provided under contract) that are not being used or are not making progress since the provision of evaluations is a use of our resources, or appear to be used incorrectly.

Legal compliance

Complying with applicable laws. Where our systems are being used, whether payment has been made or not, we process personal data in compliance with regulation and disclose such data only in accordance with applicable law. This may include making disclosures to tax authorities or law enforcement.

Legitimate interests

We may use personal information for purposes other than those shown in our privacy policy. This includes helping manage the risk for us and our customers by carrying out an assessment of our interests in using personal data against the interests of the citizen and their rights under data protection laws. The results will determine whether we can use personal data in the ways described in our privacy policy, except for marketing, which will require specific consent.

Consent

We may provide marketing information about our services or products where customers provide consent. This allows them to opt out of receiving communications that are marketing. Customers wishing to opt out of marketing communications will have that ability with every communication they receive or they may email sales@locklizard.com and ask for, but not operational emails relating to the conduct and use of our applications as covered in the previous section.

Other matters

There are categories of data defined by GDPR as sensitive data. These include medical & health, racial & ethnic, genetic and biometric, sex life & sexual orientation, criminal conviction data. Other than to comply with regulation that may require such items to be processed, Locklizard do not aim to collect or process any of these, although they may be gratuitously given to us by people filling in forms or sending us emails. The security that we apply to data received is commensurate with not processing sensitive data.
We do not use data aggregation techniques, nor do we obtain personal data from third parties other than for the processing of financial information, nor do we supply data to third parties, except where regulation requires it.

Email campaigns use opt out methods to support the principle that customers can opt out of receiving communications if they receive marketing communications that did not emanate from data that we have collected directly.

The length of time we keep personal data varies depending upon the circumstances for which those data were collected, but is never less that required by regulation for keeping accounting information or within the statute of limitations provided set out in regulation for litigation. Where a customer has purchased a perpetual license for one or more products data will be retained to allow financial history, purchases, support history and so on can be traced for the continuance of contract. In this case, data will be retained for the statutory periods after a perpetual license agreement has been revoked. Where personal information is collected during evaluations it will be retained for 18 months to detect and prevent unreasonable multiple duplicate requests or potential commercial usage. We will only retain personal information outside these timescales if there’s a legitimate and provable business reason to do so.

Customer service requests

The data that we collect from you may originate from, or be transferred to and stored at a destination outside the European Economic Area ‘EEA’ with third party suppliers, sub-processors and agents. We only transfer your data when we are satisfied that the level of protection afforded by the implementation of our applications is in accordance with this policy, or that the transfer is to a territory that is deemed adequate by the European Commission or where the recipient is subject to suitable certification and the information is subject to suitable safeguards. It is deemed that encrypted information, where Locklizard is the holder of the keying information and selection of algorithm, may be stored at any location.