Pipeliner

WHITE PAPER

CRM Security

↳ At Pipeliner, We've Got This

by Nikolaus Kimla • CEO • Pipelinersales, Inc.

TABLE OF CONTENTS

Data Security and Risk Assessment

There are many IT security concerns in the world today. This is why we've written this white-paper detailing why, when it comes to CRM, you need not have such worries with Pipeliner.

Trust

To begin with, a critical factor is trust. Who can we trust today? Trust is a word that is liberally abused, not only by governments but by many others. An example is that you trust someone who claims to be covid-vaccinated, and they're showing you a stolen vaccine card.

In the area of data, trust is extremely critical. Not only must we trust the data, but we also must secure it. There is an endless number of criminal forces worldwide engaging in the 21st-century version of piracy: that of stealing data.

In the last two weeks alone, I received several phone calls from people claiming to be Amazon representatives, informing me that my credit card had been used to purchase an iPhone 13. The "Amazon rep" says that if I have not made this purchase, they can guide me through getting the charge reversed. They do a pretty convincing job, sounding like they're from a legitimate office. Of course, they ask clever questions designed to allow them to get inside my phone. I didn't fall for it, but unfortunately there will be many that do.

Keeping Data Safe

For Pipeliner, we have chosen a very safe environment with Amazon Web Services *(AWS)*.

We have four different locations throughout the world where data is kept. This is especially important when, for legal and other reasons, data cannot be shared from one geographical location to another.

This wasn't an issue back at the beginning of the internet. Companies kept data everywhere and anywhere. But today, there is strict concern over what entities have access to data. Risk factors must be kept to a minimum.

Hackers

Today, you often must be concerned over whether the data you are receiving is correct because data can be so easily manipulated through hacking. We hear far too many stories today about profiles being stolen. This just cannot happen with SaaS companies, as their most valuable asset is their customer data.

I am constantly amazed at the sheer number of emails I receive every week, offering me customer data from my CRM competitors. I have to wonder how they're obtaining these names. This activity is not even legal, as people would have to opt-in for us to contact them.

Risk Assessment

Therefore you have to take into account numerous factors when performing risk assessment in data protection. There are many regulations and standards that must be adhered to, such as international standards **ISO 27001** and **ISO 22301**, and GDPR for Europe. Your data must be wholly segregated between clients and, as we noted above, between geographical areas. Is your technical architecture secure?

Within your company you should also ask if your employees who handle data restricted by contracts and confidentiality agreements?

Let's now take a look at why Pipeliner chose AWS as a Cloud provider to begin with.

Why AWS?

There are now several Cloud providers available, in addition to Amazon Web Services *(AWS)*. We chose to go with AWS over a decade ago and have remained with them ever since. Why have we done so? Here is our path and reasoning.

Original Data Center

Going back a couple of decades, to provide development and hosting to our banking compliance client World Check, we established our own complex data center with 50 or 60 rack-mounted Alpha and, a bit later, IBM servers. We had tremendous failover services, load balancing and backup systems. There was considerable other hardware required—server cages, routers, bridges, disk drives and high-speed cabling.

There are extensive resources required to operate such an infrastructure. We needed multiple contracts with hardware and software vendors. We had to have staff to run and care for everything in the site. People needed to be available at all times to care for equipment failure or damage, as we couldn't afford for the system to be down at any time.

Seeking Outsourcing

Throughout this time, I was always keeping my eye out for services through which we could outsource our data center. Today the whole topic of outsourcing is obvious for everyone, but back then it wasn't. Additionally I had an expensive background in running a data center, so had precise requirements.

At the time, there were very few providers of that kind of service. There was IBM, to whom we were already connected. There was Microsoft and, representing one of the large European data centers, I flew to their Dublin site and toured their enormous data

center. They actually used the cold ocean winds to cool their servers! It was quite impressive.

But Microsoft was a closed system, and I have recounted numerous times throughout my books and articles how, at the time, I was a very vocal advocate of open source. I contracted with the Austrian government to explore open source's possibilities. I ended up in a public argument with Microsoft at a press conference on the subject, as they insisted that open source would never come to pass. Fast forward some years, and in 2018 they purchased the world's largest open source repository GitHub for $7.5 billion. Microsoft totally reversed its stance, and my prediction came 100 percent true.

Partnering with AWS

We jumped on AWS right from the beginning, now 12 or 13 years ago. Many didn't know it at the time, but alongside Amazon, Jeff Bezos was also building Amazon Web Services, focused on supporting companies in easily building Cloud infrastructures.

Today, we have our production infrastructure running in 4 AWS regions: **Toronto, Sydney, Northern Virginia** and **Frankfurt**. We have a staging environment in **Dublin**, at which we can stage our application and thoroughly test it.

Going with AWS made for a considerable reduction in our efforts and costs. We didn't have to outlay money for hardware, negotiate with vendors, or hire staff to run the data center. I would say outsourcing has reduced our expenditures by 70 to 80 percent compared to doing it ourselves.

Security

Another reason we chose AWS was that they already had robust security protocols and systems in place.

Data Retention and Backup AWS provides perimeters for us to follow regarding data retention and backup. In our case, we retain customer data for a maximum of 35 days. The entire database can be recovered at any time during this retention time.

If a customer requests that their data be totally removed from our system, the live database can be removed within a day of the request. Backup data would become available following the expiration of the 35-day retention period.

Alternatively, a customer can choose to have backup data eliminated simultaneously with the live database.

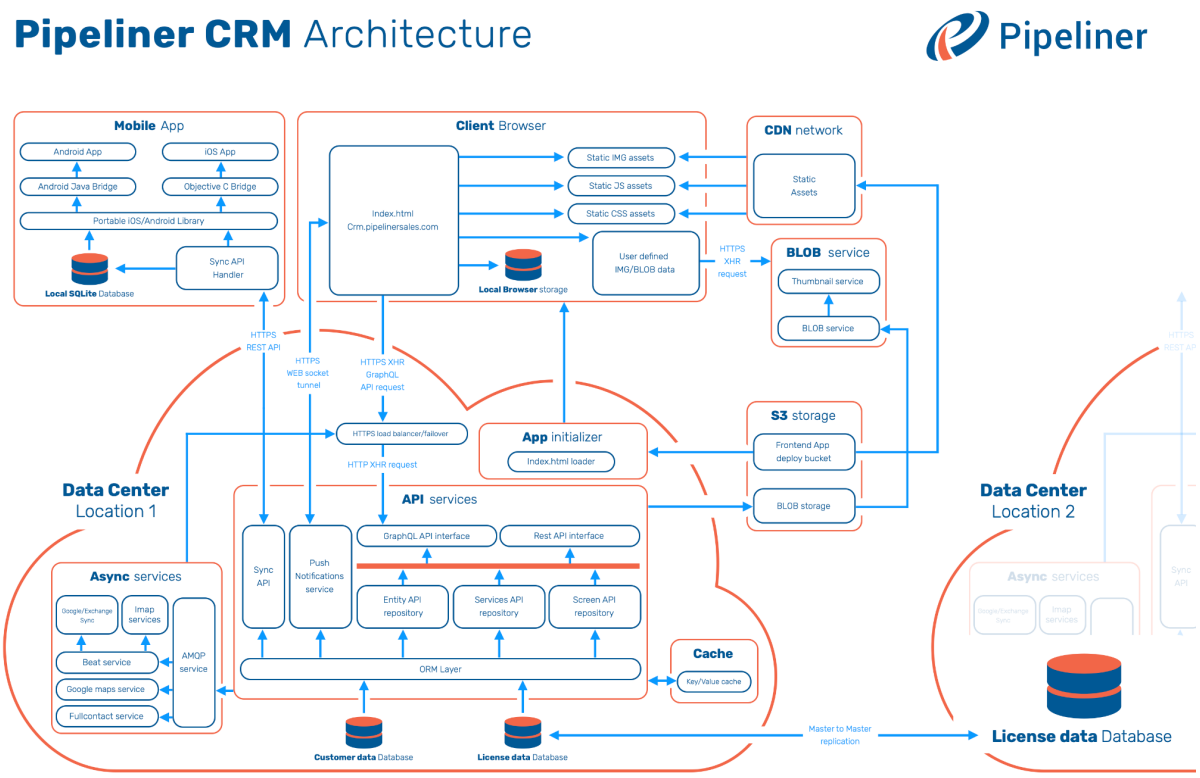
For a complete explanation of AWS data retention and backups, click here.

Data Segregation Between Clients AWS has a protocol whereby customer data is highly secure and separated, following the ISO 27001 security standard.

AWS allows the creation of a primary database instance, and then synchronously replicates it to different Availability Zones. This allows us as a CRM to have multiple data centers around the world—something not all CRM vendors offer. This means that data available to one region is not available in others. For example, European GDPR regulations stipulate that European data should not be available in North America.

Each customer space within our CRM application represents a separate database, along with a mirror of that database. If required, we can provide an additional layer of isolation. In that case, customer data would reside on a separate database server, associated with the CRM infrastructure.

Firewalls The diagram below demonstrates high-level firewall security, conducted with load-balancing WAF *(Web Application Firewall)*, IPS *(Intrusion Prevention System)* and IDS *(Intrusion Detection System)*.



If one of our customers has special firewall requirements, we can accommodate them in a separate dedicated environment.

Key and Secret Key Management For the management of private and secret keys, we utilize the AWS parameter store and encrypted Ansible Vault with audit/change log.

AWS Parameter Store provides secure, hierarchical storage for configuration data management and secrets management. Within the Parameter Store can be stored data such as passwords, database strings, Amazon Machine Image *(AMI)* IDs, and license codes.
Ansible Vault utilizes encryption for the protection of sensitive content such as passwords and keys.

Next, let’s take up overall data security management from Pipeliner.

Overall Pipeliner Data Security Management


CERTIFICATE

Today, any company seeking a CRM solution will have questions about data security, simply because data security is a top concern. Here are answers to specific questions many have about data security in Pipeliner CRM.

Limiting Data Access

Data access can be limited based on numerous factors such as types of users, groups, permissions or data elements. Task level permission can be assigned to users, and users can only view or edit specific records defined in administration. Tasks themselves can also be assigned multiple access levels.

Security is applied at field level for sensitive information—sensitive information can be hidden for selective roles. Field level security allows you to make fields invisible, enable them for read-only or for full access. There are no fields or features in our standard data model that are not configurable by the client.

Administrators set roles and permissions, and administrators themselves can be assigned various levels of privileges.

Pipeliner employees do not have access to customer data, which is part of our GDPR compliance. If a client chooses, they may add a Pipeliner employee as an authorized user and thereby grant access to the customer's data. Otherwise, we are only able to see customer usage of the system, but not the data.

Audits

So that changes can be tracked, Pipeliner maintains a log of all changes to data in the system, including the time of the action, the user taking the action, and the specific action and data changes.

Encryption of Data at Rest (AWS Amazon)

Amazon RDS encrypts your databases using keys you manage with the AWS Key Management Service (KMS). On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots. RDS encryption uses the industry-standard AES-256 encryption algorithm to encrypt your data on the server that hosts your RDS instance.

Data Encryption

Data in transit is encrypted and securely transmitted using the latest SSL *(secure socket layer)* technology. Data at rest is encrypted by our cloud provider AWS *(Amazon Web Services)*. AWS utilizes the industry-standard AES-256 encryption algorithm for the encryption of data on the server.

Pipeliner is fully GDPR compliant.

Encryption of Data in Transit

Encrypt communications between your application and your DB instance using SSL/TLS. Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when the instance is provisioned. For MySQL, you launch the mysql client using the –ssl_ca parameter to reference the public key in order to encrypt connections.

Secure Data Transmission

For the secure transmission of data via the internet, Pipeliner CRM is using the latest SSL (secure socket layer) technology. This way data is encrypted and securely transmitted to you.

Apart from encryption to secure data, Pipeliner CRM has a number of technical and organizational safety measures in place. These measures are continuously improved based on technical developments. Pipeliner CRM maintains a firewall system based on the latest state of technology, in order to protect itself from unwarranted outside access.

Encryption levels

A strong and safe 2048-bit cypher using SSL is used on all communications outside of the DMZ.

Data Backups and Disaster Recovery

As covered in our last section, CRM data is fully backed up. You can recover your database at any point during the backup retention period of 35 days, guaranteed by AWS RDS backup services. We can at any time provide a complete backup/dump of the data, and with one of our technologies, Bi-Feeder, we can even provide daily access to the full database.

We inherit the disaster and failover capabilities of the AWS environment. In addition to these, Pipeliner CRM has an internal mechanism for a secondary site to be available within 24 hours.

Login Authentication

Pipeliner has the ability to integrate its login with the client's sign-on protocol, through SAML 2. Two-factor authentication, if required, is provided by external services, such as Google or Microsoft.

Platform Configuration

A complete, easy-to-use toolkit is provided for platform configuration, defining workflow rules, automation, data visualization and more.

Forms and fields can be fully customized. Workflow rules can be fully defined through process creation, and record previews can also be customized.

Please contact us if you have further questions about our data security management.

Pipeliner CRM

Exceptional Engagement

The Better CRM › Built for Sales, Used by Sales!

TRY IT FREE or FIND OUT MORE

Pipeliner

The Pipeliner Universe — Sales Enablement, Knowledge, Networking

Pipeliner CRM
pipelinersales.com

Sales POP!
salespop.net

Go Ahead!
go-ahead.global