These were some questions presented to Adilas, LLC. on 9/20/19. Brandon Moore, the adilas lead developer responded. Answers are in blue.

1.) Where is data source stored?

The data source is a MySQL server database and it is stored on a dedicated drive inside of a dedicated server. We have multiple servers. Each server stores its own database. Our primary commercial hosting environment is with a company called Newtek. They are based out of Arizona in the USA. We are currently expanding to AWS (amazon web services) as well, this will extend our range and data storage options.

2.) What is the format of the data being stored? (Hard Copy, Electronic)

We store both hard copy items and electronic data. The hard copy pieces only deals with photos, scans, images, and other uploaded files called media/content. All other data is stored electronically in the database.

3.) If stored on a drive, where?

There are two drives per server (multiple servers). The C drive houses all application files and code. The D drive is dedicated and only holds database records.

4.) If stored in a database, what database?

The data storage engine is a MySQL server database.

5.) If stored on a server, what server?

All servers are commercially hosted machines leased from Newtek or AWS. Each is a dedicated box. We do have a couple of servers that are called a VPS (virtual private server) but most of the original servers are physical dedicated boxes. We often refer to the different servers by name (technical name known to the server company) or by number (ease of use for our backend developers and system admin persons). For example: WDEDK32 (tech name) or Data 3 (simple name). Depending on the client, the server names will change.

6.) Is the system 3rd party owned? (Y/N)

Technically, Newtek, the commercial server farm owns all of the machines and/or boxes (servers). However, Adilas, LLC. leases those dedicated boxes and we have full admin rights and privileges. Newtek is just the host and/or server farm. Adilas, LLC owns all of the data, code, and other system assets.

7.) Is the system externally hosted? (Y/N)

Yes, all servers are commercial hosted. Currently Newtek is the primary hosting company followed by AWS as an up and coming venue as well.

8.) Where is the system hosted? (UK, EU, outside of EU)

Newtek's primary location is in Arizona in the united states. They do however, have other data farms spread throughout both the US and Canada. Most of those other sites are just mirror sites. Honestly, I would need to get more information there, to my knowledge, our data only exists in the Arizona data farm.

9.) Does the third party have access into the application itself to view data? (Y/N)

Newtek is contracted to watch the main server stats, performance, operating system updates, virus protection, network issues, and hardware. All internal working of the application, data, and the adilas system are controlled by Adilas, LLC. Technically, if they wanted to, meaning Newtek, they do have full access to the servers (onsite or through admin tools). This is a huge commercial data farm. We basically assume that they are not looking at any of the stored data for any reason.

10.) Is the 3rd party a data processor? (Y/N)

Yes, Newtek is technically a data processor but we don't have any contracted services with them for data processing other than specific merchant processing accounts (setup independently). All data processing is done internally through code and process created and maintained by Adilas, LLC.

11.) Is there a Joint Controller for the data? (Y/N)

No, there is not any joint controllers on the data.

12.) How is the data collected from EU Residents? (Manual enter into website? Call employee? Receive data from third party?)

All of the above. The system is primarily setup to handle manual entry from a secured website. The website uses system permissions, logins, corporation specific checks, validation, and other logic rules to facilitate the process. There are certain processes that are automated, and data is filled in by backend processes. It is possible for someone to call and get some data entered through a phone or email request (say a tech support call or something like that). And depending on the system, we do have a number of 3rd party vendors that may supply data back and forth. All 3rd party vendors must be turned on physically, from inside the system, by an administrator, before any transactions are possible. The primary way we get data is through manual use of the secured website and/or application.

13.) Is consent taken from individuals? (Y/N)

This question seems very open ended. Yes, we do try to listen and talk to individuals. No, we don't ever just change things based on a request. If that is needed, it goes in writing and we, on our side, get permission and authorization from system admin persons to do such actions. We have options of recording histories, and making sure everything is tight including scans, screenshots, and other supporting files (uploaded media/content). We then record and document those proceedings. In general, the system becomes the boss and only users with specific permissions are permitted to do certain actions.

14.) Is data or a portion of the data sent to other places? If so, where? (Other departments, other office locations, around the world? etc.) (Y/N)

Technically, yes, some of the data is sent to other places. All internal data is sent from dedicated servers to other dedicated servers within the adilas network. Most of the data that we collect and send to other servers deals with inventory items. These may be of two types – serialized stock/units or more general items or widget based inventories. The primary purpose for this is an outside web presence to show items and inventory for sale (called ecommerce or web presence). It is also important to note, that certain pieces of data are held and maintained in master lists. In that case, data from a smaller dedicated box would report to the master data server in order to main system wide lists and other master type lists.

The other thing to note here is that individual companies and/or corporations may turn on/off and allow outside 3rd parties to interact and participate in some sort of data sharing. This could be for outside state compliance services, mandatory monitoring processes, special sales and marketing firms, analytics, promotions, text and email communications, product reordering, or some other service. Once again, each company is allowed to interact with whom every they choose, if it goes through the 3rd party solutions section

within Adilas. Once the data is passed between the adilas servers and the 3rd party, we take no further interest in what happens to the data from there.

By default, all virtual windows and doors are closed and sealed unless a company specifically turns on/off a 3rd party solution. That puts the power of their data into the hands of our user corporations. We just offer the services; they choose how to consume those offerings.

15.) How is data transferred from the source? What method is used for transfer? (email, secure file transfer, hard copy)?

Most of the data and reporting is done through the secure website and application portal. The actual website has extensive permissions and processes in place. Our protocol is to let the companies have access to their data. If they want to print, email, convert to PDF, export as Excel or CSV (comma separated values), or some other format, we allow that. Once the data is displayed, the use of that data falls upon each user and/or company.

It may also be important to note that Adilas does have and supports an API (application programming interface) socket interface. An API socket interface allows for raw data to be pushed and pulled based on valid credentials. By default, all virtual windows and doors are closed and sealed. Company administrators are able to virtually open and close those API socket doors and windows through an admin interface. Once an API socket window or door is open, we do track who requests the data, and how often, but we have no way of knowing who the consumer is other than tracking the requesting person's id and their IP address. There are extensive checks and balances, but an API socket is what it is, it is an open raw exchange of data based on requests and valid credentials.

16.) Is the personal data protected at rest?

The answer here is yes. Most of the data in the database is stored in normal human readable format (numbers, strings, dates, id's, etc.). Anything that we consider to be sensitive data (username, passwords, bank accounts, license numbers, SSN's, account numbers, merchant processing keys, etc.) are all encrypted for storage (non-human readable). There are other things that are hashed (scrambled) and/or URL encoded (substituted) for storage. At rest, the data should be very protected.

17.) Is the data backed-up?

Nightly back-ups of the database and the code are done. Those data back-ups are stored off-site and have a rolling 2-week cycle. As part of the back-up process, we allow our users to pull and make their own back-ups. This empowers the users and the different corporations to have a hand in their own back-ups. This could be normal web reports, PDF documents, Microsoft Excel spreadsheets, CSV files, uploaded files, and other documents.

18.) Estimate the Total Number of Data Subjects: (<100, 1000+, 10000+, etc.)

As of today's date, 9/20/19, the total number of data subjects (meaning clients) is between 350 and 1,000 companies. Those companies are spread over 15 dedicated servers with thousands and thousands of users. Millions and millions of transactions and induvial data records are being stored. Each database has no less than 200+ tables. There are millions of fields, and millions of records.

19.) Is the personal data deleted? (Y/N) If yes, how? (deleted, overwritten, shredded)

No data is deleted unless a specific request is made in writing and documented. Our general practice is all data is live and searchable. We do use a number of status fields, that allows us to show/hide and make things active or inactive, but as a general rule, we do not delete any data. The only exception to this, is if we are purging an entire system out of the database. That is very rare. Our most common practice is to turn things off and make them inactive. Most of the secured website code operates on active data only. All other data is virtually hidden.

20.) How long is data retained? (indefinite, 7 years, other)

The rolling back-up is retained off-site for a 2-week rolling cycle. All other data is retained for life unless we have specific requests to delete and/or expunge that data. A user is unable to delete any data whatsoever. They are only allowed to show/hide and set the status of certain items and data pieces. As the users interact with the system, locked history records are recorded and available for view within the system (internal audit trail). Only adilas developers can do anything of consequence to live data. There are log files on the actual servers that watch and monitor the servers (from the backend). Most data is retained for life.