AiFi GDPR Whitepaper

Version of March 2024

Version V 2.5

This GDPR Whitepaper has been approved by the board. This document will enter into force as of September, 2023 (Effective Date).

Content

Foreword

We at AiFi Inc. are committed to protecting privacy. This GDPR Whitepaper describes the way we process personal data as a data processor on behalf of our clients (the data controllers) through our services, where such processing of Personal Data is subject to the GDPR[1].

AiFi processes Customer Data (including personal data as processor) under the direction of our clients. AiFi has no direct control or ownership of the Personal Data we process on behalf of our clients. Clients are responsible for complying with any regulations or laws that require providing notice, disclosure, and/or obtaining consent prior to transferring the Personal Data to AiFi for processing purposes. Terms not otherwise defined herein shall have the meaning as set forth in the General Data Protection Regulation (GDPR).

We periodically update this GDPR Whitepaper. AiFi may supplement this GDPR Whitepaper through policies, standards, guidelines, and instructions that are consistent with this GDPR Whitepaper.

AiFi Services, processing of personal data & data flow

The services

AiFi is a software company specialized in the development of innovative software solutions for the retail industry. AiFi provides two services, the AiFi Auto-Checkout Solution OASIS and the NanoStore®. Both services incorporate the AiFi Data Annotation and Training (hereafter: “DAT”) service.

Auto-Checkout and Security Solution OASIS

The AiFi Auto-Checkout Solution OASIS is a suite of advanced hardware (Camera’s and/or Shelf sensors) and software (A.I. Algorithm) powered by AiFi’s proprietary computer vision and sensing technologies.

[1] This GDPR Whitepaper does not apply to any information or data collected by AiFi as a controller for other purposes, such as information collected on our websites or through other channels for marketing purposes.

The AiFi Auto-Checkout Solution (OASIS) provides the shopper with a frictionless checkout-free shopping experience. It also enables retailers towards secure (identifying possible security incidents) autonomous stores with operating efficiency, extended operation hours, better user experience and full digital awareness.

NanoStore

The NanoStore is a complete solution in a box - a fully automated, container sized, checkout free store. It is shipped directly and ready to deploy. We are able to deploy an entire fleet of stores in only a few days. The NanoStore runs on AiFi's proprietary OASIS platform.

DAT Service

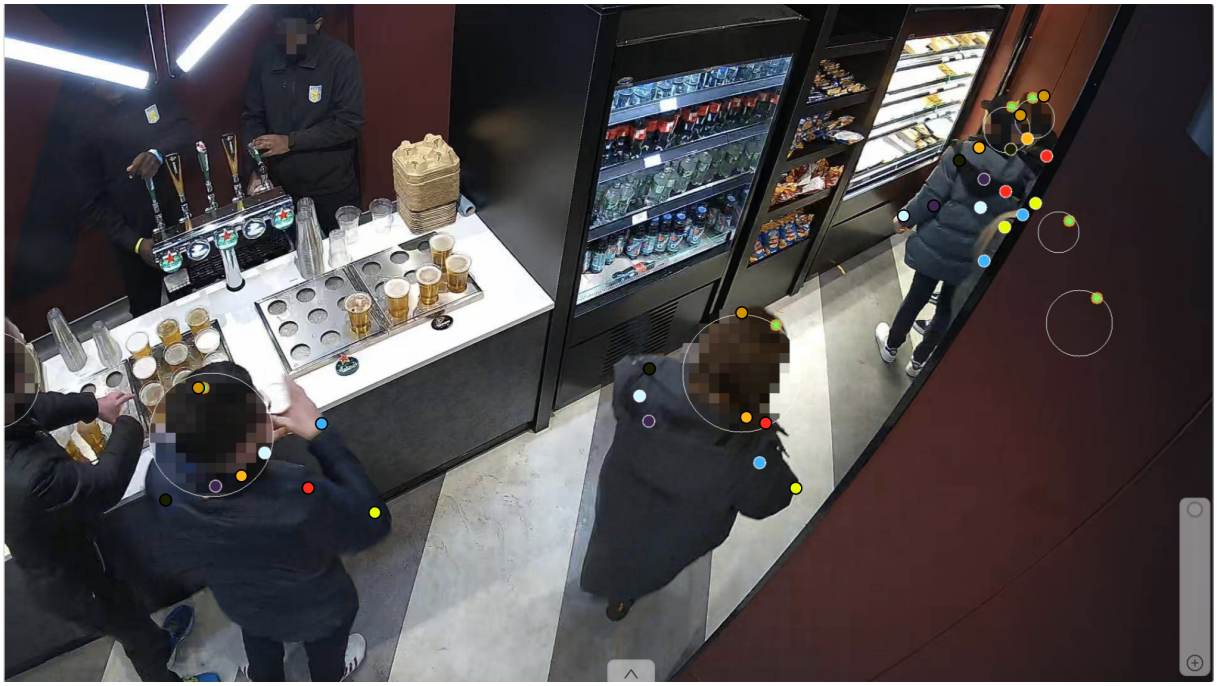
The AiFi OASIS system continuously makes calculations of the probability regarding a selected item by the shopper. If the probability goes below a certain threshold, the DAT service provides human assistance in determining which product is selected by the shopper.

The DAT agent augments the OASIS technology systems to execute and/or correct a cashierless checkout transaction with shoppers. The OASIS system provides blurred video snippets (of 5 – 8 seconds long) to the DAT agent in order to determine which product is selected and provides the DAT agent to augment the shopping basket in real time.

AiFi can also provide an additional DAT function to review contested receipt post-transaction. In that case the DAT agent reviews the contested item on a receipt based on a blurred video snippet to determine if the shopper contested the receipt rightfully. Depending on the scope of the service, the DAT agent could change and

adjust the receipt if the outcome of the review is that the contested receipt was rightfully done by the shopper.

The DAT component is also used to improve the on prem AI. Video is transferred only from the on prem to the AiFi cloud for the DAT cloud component, and all detected faces are blurred before being transferred out of the on prem network.



Video for DAT is stored for at most one week and is transferred over the VPN via a Kafka broker, which is a message broker system that allows data to be passed between services through it.

Processing (personal) data with OASIS and DAT

OASIS combines sensors, cameras and sophisticated software to create a state-of-the-art automated retail solution. OASIS achieves superior shopper tracking with only a minimal number of RGB cameras as compared to other systems which require hundreds of expensive depth cameras. AiFi does not use facial recognition or collect biometric data[2] for identification purposes.

The OASIS system consists of the use of cameras, the DAT function and AI software. Every time a shopper enters an OASIS implemented retail store, the OASIS system

[2] "'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data". The OASIS system does not use the video footage to identify a natural person as the footage is only linked to a random token ID (video footage is not enhanced with facial recognition). Therefore, the system is not processing data to identify individual shoppers.

creates a unique token for and tokenized stick figure of the shopper and attributes a virtual shopping card to the tokenized shopper in order to keep track of the items the shopper picked-up during his or her visit to the retail store. This tokenized stick figure is tracked throughout the store to assist the OASIS system in recognizing the picked-up items. If the shopper leaves the store without picking-up any items, then all data is instantly deleted.

The cameras used for the OASIS system only capture information from inside the store. All information from outside the store is instantly blurred.

If a tokenized shopper picked-up an item, the OASIS system calculates the probability that the selected item is recognized correctly. This is done by using the tracked location of the tokenized shopper and combining that with the product recognition abilities based on the video footage and AI software.

If the OASIS system doesn't reach a probability score threshold of an item or if the shopper contests an item on their receipt, a short video snippet of five - eight seconds for each event in which the shopper is blurred and shown to pick-up a certain item, is pushed towards the DAT operations team to verify the picked-up item and/or alter the receipt. The DAT function also helps to improve the AI of the OASIS system.

Depending on the set-up of the store, the shopper can walk out of the store and the pick-up items are automatically charged to their credit card or pay for the items at a payment terminal.

The OASIS system doesn't require any additional personal data, such as name, address, customer number, credit card number, et cetera to provide the frictionless shopping experience.

The in-store events (items picked up, placed back et cetera) and tracking, the virtual basket, product information, technical information and movement of the stick figure and blurred video snippets are all attributed to the unique token, created for that specific shopping experience. The OASIS system will not be able to recognize if the same data subject enters the store for a second time as for every visit to the store, a new unique token is created.

Where is personal data being processed?

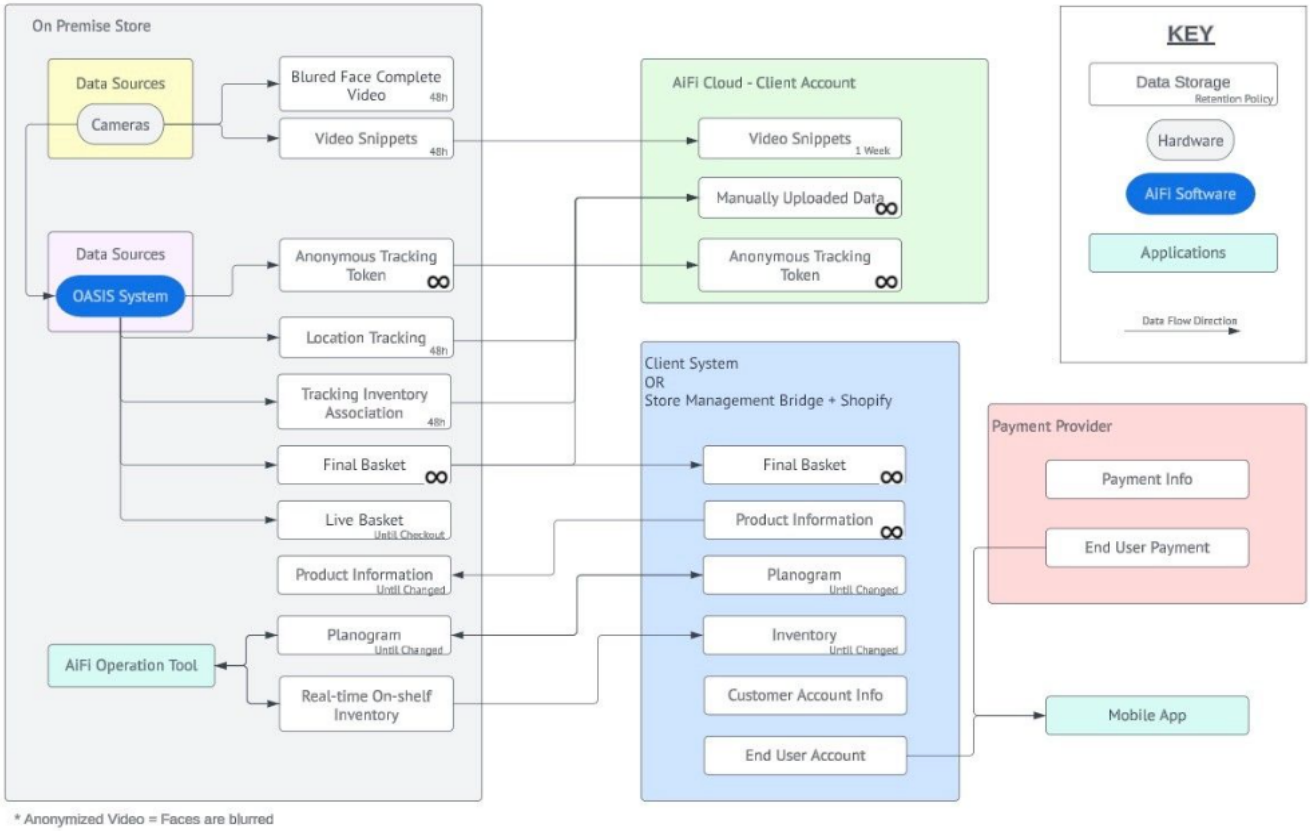
AiFi let's its clients be in control of all personal data processed of the shoppers. An important key element is that the OASIS system runs on-premise. Most of the data is processed inside a store for maximum security (as shown in the data flow below). Therefore, there is a distinction in processing activity and purpose between the personal data processed by the OASIS system on premise (and to which personal data the client, as data controller has access to) and the personal data processed by AiFi in the AiFi cloud.

In the data flow there are four different locations that play a key-role in the processing activities of personal data through the OASIS system: i. on premise, ii. the AiFi Cloud, iii. the client system (or the store management bridge) and iv. the payment provider. Please note, the payment provider processes personal data as data controller and no financial information is shared between the payment provider and AiFi or the OASIS system.

Raw video data from the cameras are processed and (almost) instantly blurred on premise[3]. The OASIS system automatically blurs the entire head of every shopper that enters a store.
Furthermore, to comply with the data minimization principle and to ensure no personal data is processed of data subjects outside the store, the OASIS system can optionally also provide a so-called "blurring curtain" that blurs all video footage from outside the store or site boundary. For example, by blurring all video footage from windows, (glass)doors or indicated location boundaries. All blurring is automatically executed on premise and requires no additional human involvement. The client is responsible for its Client system or store management bridge and connection to a payment provider.

[3] No raw video data is uploaded to the AiFi Cloud, unless specifically agreed upon with our clients, for example for specific research and development purposes.

Figure 1 – data flow on-premise <> AiFi Cloud <> Client system and Payment Provider



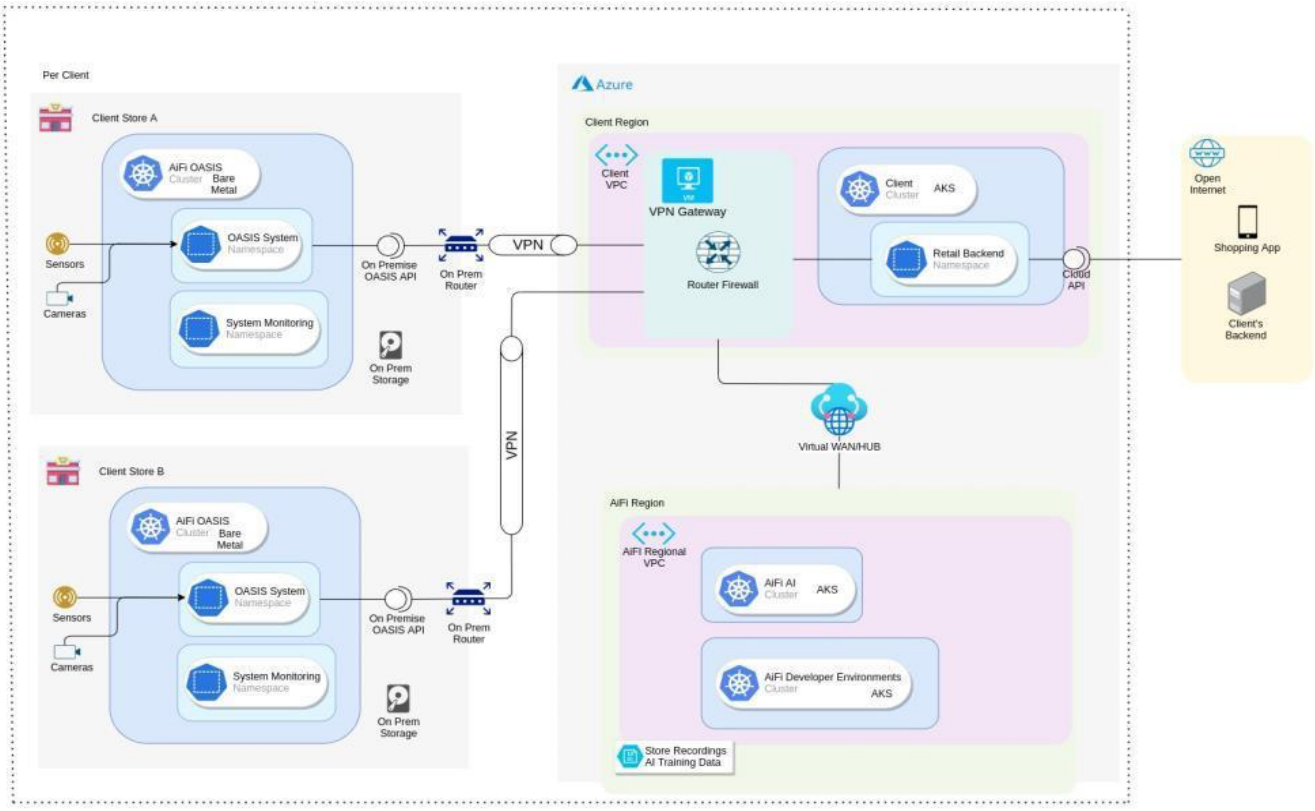


Figure 2 – high level architecture data storage

On Prem

On prem services reside in a local bare metal Kubernetes cluster on the same LAN. Cameras and sensors also reside on this LAN. All machines are behind a router firewall. Remote access is controlled via SSH keys and Kubernetes cluster credentials.

SSH keys and Kubernetes cluster credentials are stored in the Azure Key Vault which has its access controlled via Azure AD. On prem router logins are stored in a controlled BitWarden group. The on prem router is connected to a per client VPC on Azure.

Clients on the LAN can access machines and hardware on the network if they have the proper credentials for SSH, RTSP, or the Kubernetes control plane. Clients on the VPC can only access select exposed on prem machines if they have the proper credentials for SSH or the Kubernetes control plane. On prem API requires an API key to be used. The API allows access to the store's layout, planogram, and non-identifying shopper information.

Non-identifying shopper information is the randomly assigned shopper ID used only for instore tracking, the trip session the shopper is assigned to, and the retailer IDs of any products/objects the shopper left the store with. The API does not allow access to either the shopper's tracked skeleton or any video.

On prem routers are connected to cloud virtual routers via OpenVPN hosted on Azure Cloud in a client specific VPC. Credentials for these VPN connections are per store and are stored in a controlled BitWarden group. Stores connected to the same client VPN are isolated via router firewall.

AiFi Cloud

All client store networks and client-related cloud services are contained in a client-based fully isolated VPC on Azure. AiFi engineers can only access this cluster via Azure VPN Gateway and if the engineer has the correct Azure AD permissions to access this cluster. The cloud -hosted API is SSL terminated and certificates are managed internally to the cluster as Kubernetes Secrets.

Only engineers with both access to the cluster and further permissions to view Kubernetes Secrets can see these certificates. Server certificates are signed by Let's Encrypt and last for 30 days. The cloud API requires an API key to be used. This API allows access to all of a client's store layouts, planograms, and the retailer IDs of any products/objects that were in shopper baskets group by receipt. The API does not allow access to either the shopper's tracked skeleton or any video.

Default Retention Period Schedule

The client (as data controller) is responsible for determining the retention schedule for all personal data processed on-premise and in the AiFi cloud. However, AiFi provides a default retention schedule for the data stored in the AiFi Cloud:

CATEGORY OF DATA	**DEFAULT RETENTION PERIOD**					
	Execution Agreement – providing services	*Improving Ai and DAT (Accuracy function)*	*DAT – contested item on receipt (if outsourced to AiFi)*	*Problem solving (maintenance and support)*	*Storage*	*Analytics*
Raw video	On Store Storage - 48 hour	N/A	N/A	Limited (only access when necessary to solve problem).	1 week	N/A
Video snippet	On Store Storage - 48 hours On cloud storage – 1 week	N/A	Limited (only access when necessary for DAT function)	Limited (only access when necessary to solve problem).	1 week	N/A
Video snippet without metadata (R&D)	N/A	2 months	N/A	Limited (only access when necessary to solve problem).	N/A	Limited (only processing data during anonymization process).
Location and date	On Store Storage - 48 hours On cloud storage – 1 week	N/A	N/A	Limited (only access when necessary to solve problem).	Receipt data for fiscal/administrative purposes is stored (by default) for 1 year.	Limited (only processing data during anonymization process).
Tracking token	On Store Storage - 48 hours On cloud storage – 1 week	Limited (only processing data during anonymization process).	N/A	Limited (only access when necessary to solve problem).	1 week	Limited (only processing data during anonymization process).
Technical (and sensor; RFID [Radio Frequency Identifier], and weight sensors) data	On Store Storage - 48 hours On cloud storage – 1 week	Limited (only processing data during anonymization process).	N/A	Limited (only access when necessary to solve problem).	1 week	Limited (only processing data during anonymization process).
Third party devices [e.g. coffee machine; vending machine]	On Store Storage - 48 hours On cloud storage – 1 week	Limited (only processing personal data during anonymization process).	N/A	Limited (only access when necessary to solve problem).	1 week	Limited (only processing data during anonymization process).

Product information	On Store Storage - 48 hours On cloud storage – 1 week	Limited (only processing data during anonymization process).	Limited (only access when necessary for DAT function).	Limited (only access when necessary to solve problem).	Receipt data for fiscal / administrative purposes is stored (by default) for 1 year.	Limited (only processing data during anonymization process).
Virtual basket information	On Store Storage - 48 hours On cloud storage – 1 week	Limited (only processing data during anonymization process).	Limited (only access when necessary for DAT function).	Limited (only access when necessary to solve problem).	Receipt data for fiscal / administrative purposes is stored (by default) for 1 year.	Limited (only processing data during anonymization process).
Movement of tokenized stick figure	On Store Storage - 48 hours On cloud storage – 1 week	Limited (only processing data during anonymization process).	N/A	Limited (only access when necessary to solve problem).	1 year	Limited (only processing data during anonymization process).
Tracking to inventory data	On Store Storage - 48 hours On cloud storage – 1 week	Limited (only processing data during anonymization process).	Limited (only access when necessary for DAT function).	Limited (only access when necessary to solve problem).	1 year	Limited (only processing data during anonymization process).

Processing of personal data in AiFi Cloud

Personal data transferred to the AiFi Cloud is processed for specific purposes. Below we have described the processing purposes (including an explanation), the data involved for each processing purpose and if AiFi could have access to the data stored in the AiFi cloud and if so, the reason and circumstances for access.

Purpose	Explanation	Data	Access
Improving the AI and DAT (Accuracy function)	In order to review a picked-up item due to not reaching accuracy threshold. Anonymized data and technical data are used for training purposes. All time stamp (and if applicable location data) is removed.	Anonymized video, tracking token, sensor data, movement of tokenized stick figure, item information, tracking to inventory data, virtual basket information.	For this purpose, no Personal Data is being processed. The training data is used for improving the AI and will become a part of the AI data.
DAT – contested item on receipt (if outsourced to AiFi)	In order to review a picked-up item in case of a contested item by shopper.	Blurred video snippets, (live) basket, receipt items and picked up items.	Temporary and only if the OASIS system indicates that the DAT agent should review.

Problem solving	If the OASIS system encounters downtime or technical problem and AiFi needs to resolve the fault in the system	Anonymized video, tracking token, sensor data, movement of tokenized stick figure, item information, tracking to inventory data, virtual basket information and all other technical data that could be required	AiFi will only have access to the data during the time the problem is not solved.
Storage	If the local store facilities are unable to provide sufficient storage for raw video, AiFi can provide storage at the AiFi cloud.	Video is automatically blurred on premise before its uploaded to the AiFi cloud. Blurred video is stored. All data, tracking stick figure (uploaded in cloud later).	AiFi will only store the data for this purpose and will not process it in any other way. AiFi will only gain access on request of the retailer, for example to delete the data or to send a copy of the data to the retailer.
Analytics	In the near future retailers can use the OASIS system for analytics purposes. AiFi will provide a dashboard with analytics based on the specific preferences of the retailer.	Anonymized video, anonymous tracking token, sensor data, movement of tokenized stick figure, item information, tracking to inventory data, virtual basket information and all other technical data that could be required.	Processing data only for creating a dashboard. Limited access for AiFi employees, only for problem solving. Aggregated / de-identified/ anonymized data will be used by AiFi for benchmark purposes.

Personal data processed in the AiFi cloud is always stored within the EEA. Therefore, the default setup doesn't involve any data transfers outside the EEA. However, data transfer could happen in two specific situations, as described in the following chapter of this document.

Customer Shopping App <> Cloud API

AiFi provides a White Label App for retailers. The Shopping app can be used by retailers to provide shoppers with receipts and QR codes for store entry.

If a shopper signs up with the AiFi customer shopping app, then the AiFi cloud API will have access to the following information:

- name and surname (which can be excluded on retailer request)
- email (used to log in, stored in plaintext)
- password (used to log in, stored in irreversible hash)
- payment token (only if AiFi handles payments)

Data Transfers

The GDPR allows transfers of personal data to a third country outside of the EEA if the transferring party has provided appropriate safeguards and ensured that enforceable data subject rights and effective legal remedies are available for data subjects.

In principle, all personal data of our European Clients is solely stored in the EU. The AiFi Cloud Infrastructure is located in Frankfurt, Germany (Germany West Central). However, temporary data transfers could occur for two processing activities: i. maintenance and support by the AiFi Tech-Ops team, or ii. to provide the DAT function.

i. maintenance and support by the AiFi Tech-Ops team

Due to the extended opening hours of AiFi powered stores or locations (sometimes opened 24/7), AiFi could at any time be required to provide support or maintenance.

The first point of contact to provide support or maintenance for European clients will be the European Tech-Ops team. If the European Tech-Ops team is unavailable or unable to provide a swift solution, the American Tech-Ops team will step in to quickly solve any issues.

Only in that situation will data be processed outside the EEA (more specifically in the United States) for a limited amount of time (only during the time needed to solve the problem).

It is important to note that the American Tech-Ops team will only have limited remote access to solve a problem after which access to the data will be revoked for the American Tech-Ops team. Data is never stored outside the EEA for maintenance or support.

ii. *to provide the DAT function*

Due to the growth of the number of opened stores, additional DAT capacity is required. AiFi has outsourced DAT Operator capacity to IGT within the EU, but also outsourced additional DAT Operator capacity to IGT and Fusion outside the EEA.

Due to this growth in stores, in comparison to the limited increased amount of revenue, keeping the DAT operations within the EU is financially unsustainable. Moving out of the EU to locations like India present savings in the regions of 50% per transaction enabling long term success of the platform whilst maintaining operational excellence.

Therefore, AiFi has reviewed several options (within, but also outside the EU) for outsourcing additional DAT capacity in order to ensure continuity and keep its operations profitable. Multiple factors were taken into consideration in the search

for additional DAT capacity. For example, GDPR compliance, possibility to scale, price, technical and organizational measures, experience with handling personal / confidential data.

All options within the EU and competitors of importer outside the EU could not provide the same level of IT security, price, scalability, GDPR compliance and experience. Therefore, there currently is no alternative for providing a scalable, financially sustainable solution.

There is no direct client interaction and the data displayed to the DAT agent is minimized. As mentioned, the OASIS system provides blurred video snippets (of 5 – 8 seconds long) to the DAT agent in order to determine which product is selected and provides the DAT agent to augment the shopping basket in real time.

Additionally, in terms of operational hours having a second site in a different time zone enables the ability to align normal working hours to more operators as well as offering a contingency element should there be any technical or political issues arise. Escalations will be maintained within the EU where training and quality control is managed.

Documentation is key for compliance after Schrems II.

AiFi uses Standard Contractual Clauses as basis for the data transfer from the EEA to the US. The SCC's are part of AiFi's model data processing agreement. If the data processing agreement of a client is used, then the SCC should always be added as an appendix to the data processing agreement.

The Schrems II case gives reason to address the SCC mechanism and provide additional information for our clients[4]. This means that all transferring parties (AiFi as processors and our clients as data controller), have a responsibility. This requires a risk assessment by the parties involved in the transfer, a so-called Transfer Impact Assessment ("TIA").

AiFi drafted a TIA to facilitate the aforementioned data transfers outside the EEA for both processing purposes to AiFi or IGT / Fusion. Together we must verify on a case-by-case basis (where appropriate in collaboration with the extra-EEA recipient of the personal data) whether the laws of the third country to which the personal data are transferred offer adequate protection in line with the requirements of EU data protection law[5] and if the additional measures taken are sufficient.

---

[4] The CJEU declares that the SCC (as laid down in Commission Decision 2010/87) are valid as a mechanism but cannot be regarded as a 'tick the box' exercise because the rights offered to EEA data subjects abroad should be, at least, at an equivalent level to those guaranteed under the GDPR.

[5] The way that the legal framework in the country where the recipient is established works may lead to a need to provide additional safeguards in addition to those documented in the SCC. The CJEU requires a case-by-case review whether the laws of the third country in which the recipient is

Technical and organizational measures

AiFi has implemented and will maintain appropriate technical, physical and organizational measures in line with its Information Security Policy and as described in the template DPA. These measures take into account the nature, scope and purposes of processing as specified in this GDPR Whitepaper and / or the Services Agreement and are designed to protect Customer Data from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access during the Processing.

AiFi shall in any event implement and maintain the Security Measures as specified in the DPA template, which may be revised by AiFi without notice to the clients, provided that such changes do not in any material manner diminish the level of security.

However, security is a joint effort. For example, the client is responsible for ensuring the physical security of the server by placing it in a locked, secure environment. In case of a security breach, all the hardware is protected.

On premise services reside in a local bare metal Kubernetes cluster on the same LAN. Cameras and sensors also reside on this LAN. All machines are behind a router firewall. Remote access is controlled via SSH keys and Kubernetes cluster credentials. SSH keys and Kubernetes cluster credentials are stored in the Azure Key Vault which has its access controlled via Azure AD.

On-prem router logins are stored in a controlled BitWarden group. The on-prem router is connected to a per client VPC on Azure. Clients on the LAN can access machines and hardware on the network if they have the proper credentials for SSH, RTSP, or the Kubernetes control plane. Clients on the VPC can only access select exposed on prem machines if they have the proper credentials for SSH or the Kubernetes control plane. On prem API requires an API key to be used.

Data Processing Agreement

AiFi shall Process Customer Data only based on the applicable data processing agreement that meets all the requirements under GDPR. AiFi will always provide its template data processing agreement to a potential client during the contract negotiations. Processing of Customer Data can only start after a data protection agreement is signed by both parties.

Upon termination of the Services, AiFi shall fulfill its obligations to the client in the Master Service Agreement with regard to the return of Customer Data by providing to the Client the Customer Data required for the continuity of the business activities of the client (if the data has not been previously provided or made accessible to the

established respect data subject rights at a similar level as the GDPR, including by allowing for judicial review where the authorities have access to the personal data, e.g. for intelligence purposes.

Client via relevant product functionality, such as the ability to download the Customer Data).

When AiFi's obligations under an agreement, for example a statement of work, have been fulfilled, AiFi shall securely destroy remaining copies of the Customer Data, and (upon request of the Client) certify to the client that it has done so. AiFi may maintain a copy of Customer Data to the extent required under Applicable Law, as authorized by the Client, or as needed for dispute resolution purposes.

AiFi shall no longer process that Customer Data, except to the extent required for the aforementioned purposes or in case the Customer Data is no longer considered personal data due to the anonymization of such Customer data. AiFi's obligations of confidentiality under the related agreement will persist for as long as AiFi maintains a copy of such Customer Data.

Sub-processors

The AiFi uses Sub-processors in the regular performance of the Services. The data processing agreement between AiFi and the client shall authorize the use of such Sub-processors, provided that AiFi remains liable to the clients for the performance by the Sub-processors in accordance with the terms of the data processing agreement and applicable law.

Sub-processors may process Customer Data only if the Sub-processor has a binding contract with AiFi. The contract shall impose the same level of data protection and security-related Processing terms on the Sub-processor as those imposed on AiFi by the Services Agreement and/ or data processing agreement and this GDPR whitepaper, especially regarding (timely) reporting possible data breaches, technical and organizational measures and the handling of data subject requests.

AiFi shall include a list of the Sub-processors involved in the performance of the relevant Services in the Data Processing Agreement. This overview shall be regularly updated to reflect changes. AiFi shall provide the option to Clients to be notified of any intended changes to the lists of Sub-processors engaged by AiFi for the delivery of the Services. The data processing agreement between AiFi and a client provides the timelines of such notification and the response time and consequences of client. Clients may object to the involvement of such Sub-processor in the delivery of the Services, providing objective justifiable grounds related to the ability of such Sub-processor to protect customer data or comply with applicable data protection or security requirements.

In the event the objection is not unreasonable, AiFi and the client will work together in good faith to find a solution to address such objection, including but not limited to reviewing additional documentation supporting the Sub-processors'

compliance or making the Services available without the involvement of such Sub-processor. A list of current sub-processors is added to the template DPA.

Privacy by design

Article 25 specifies that the controller, our client, has the responsibility for complying with data protection by design and by default. Article 25 does not mention data processors (like AiFi) specifically. However, Article 28 specifies the considerations our clients must take whenever you are selecting a processor. For example, our clients must only use processors that provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

This requirement covers both data protection by design in Article 25 as well as the security obligations under Article 32. AiFi cannot necessarily assist its clients with the data protection by design obligations (unlike with security measures), however they must only use processors that provide sufficient guarantees to meet the GDPR's requirements.

Therefore, AiFi will adapt certain privacy by design considerations when creating new products and services as well as functionalities to the existing products and services. Data protection by design is ultimately an approach that ensures AiFi to consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

AiFi will:

- put in place appropriate technical and organizational measures designed to implement the data protection principles effectively; and
- integrate safeguards into the processing of personal data so that AiFi can meet the GDPR's requirements as a data processor and protect individual rights of data subjects (inter alia when handling data subject requests and complaints).
- integrate data protection into our processing activities and business practices, for example by means of this Privacy Information Document, training and awareness and checks and balances.
- when developing new IT systems, services, products and processes that involve processing personal data, assess if such new system, service, product and/or process could lead to an infringement of the GDPR for client and complies with the data processing principles of the GDPR;
- developing organizational policies, processes, business practices and/or strategies that have privacy implications;
- adjust the products, services, systems and processes if a client (as data controller) or Supervisory Authority, providing objective justifiable grounds, requires a change necessary to maintain compliance with the GDPR.

Data breaches

How we deal with data breaches and which data breaches must be reported to our client, is set out and described in AiFi's Incident Response Policy. Different situations and scenarios are described, including information on how to act in such a situation, in order to mitigate risks and limit any damage.

Where AiFi becomes aware and determines that personal data has been subject to unauthorized processing (including by an employee) that compromises the confidentiality, integrity or availability of such Personal Data, AiFi will report such Data Breach without undue delay to the client to the extent permitted by applicable law and as agreed upon in the data processing agreement between AiFi and our client, in line with the process described in the internal AiFi Internal Incident Response Policy.

The GDPR includes an obligation for our clients (as Data Controllers) to report data breaches to their local Supervisory Authority. This also includes Data Breaches that occur at AiFi (or our sub-processors) that impact customer data. In order for our clients to make a timely assessment to determine if a specific Data Breach should be reported to their local Supervisory Authority, AiFi needs to make sure to:

1. train staff how to recognize and report breaches;
2. have a process to enable staff to report breaches to the appropriate individuals as soon as they become aware of them;
3. put mechanisms in place to report any breaches to the controller (our clients); and
4. monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.

What information must a breach notification to the client contain?

When reporting a breach, AiFi will provide:

1. a description of the nature of the personal data breach including, where possible:
2. the categories and approximate number of individuals concerned; and
3. the categories and approximate number of personal data records concerned;
4. the name and contact details of the data protection officer (if the client has one) or other contact point where more information can be obtained;
5. a description of the likely consequences of the personal data breach; and
6. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The GDPR recognizes that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So, Article 33(4) allows our clients to provide the required information in phases, as long as this is done without undue further delay.

However, AiFi will prioritize the investigation, give it adequate resources, and expedite it urgently. AiFi must still notify the client of the breach when we become aware of it and submit further information to the client as soon as possible.

Data subject rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Responsibility for complying with a data subject request regarding the aforementioned rights, lies with the controller, our clients, see article 28 sub 3 e[6] GDPR. Our clients need to ensure that they have contractual arrangements with us in place to guarantee that data subject requests are dealt with properly, irrespective of whether they are sent to the client or to us.

However, AiFi will have a process in place: i. in case we receive a data subject request from a shopper and/or ii. our clients, in order to provide an adequate response within the agreed timeframe of the SLA towards our clients.

Furthermore, AiFi needs to make sure all sub-processors that process personal data are aligned so they can meet the timeframe and requirements regarding data subject request, agreed upon in the SLA between AiFi and our clients.

1. [6]*taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights.*