



# SAFR SCAN

Introducing SAFR's Face Recognition Access Control system. SAFR SCAN is an entirely frictionless experience that allows users to naturally walk to the door, and in real-time use your face as your credentials. SAFR SCAN will quickly authenticate you against a database of 20,000 images. It's simple, intuitive, and secure. SAFR Scan easily integrates with any access control solution which ensures a quick and cost-effective installation. Maintain a secure environment while giving users the peace of mind that comes with never having to remember their key card.



Mobile enrollment



OSDP/Wiegand



Tailgating detection

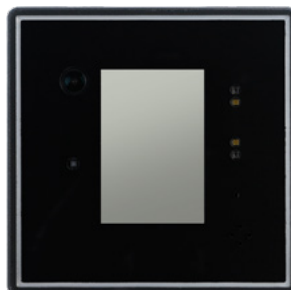


Works outdoors



Anti-spoofing

## SAFR SCAN Overview



Waiting



Alert



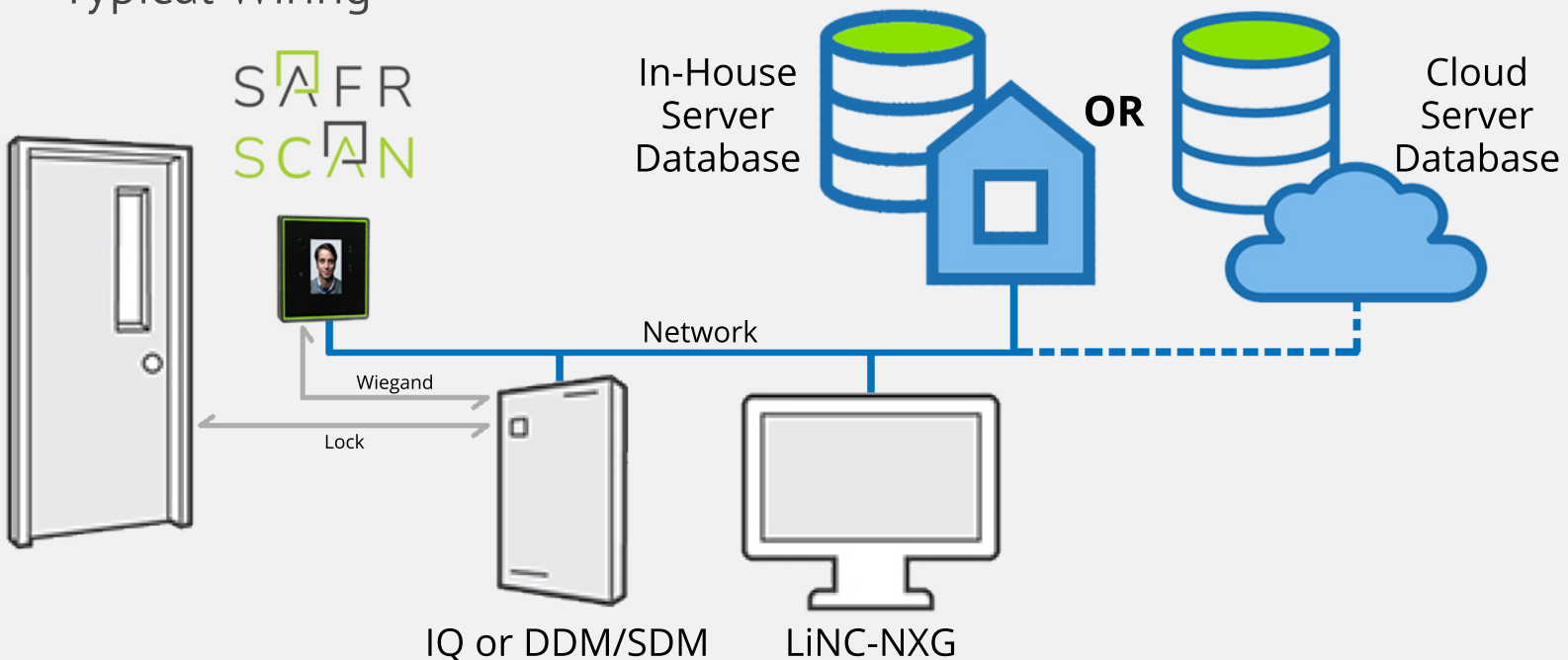
Good to go

# SAFR SCAN Key Features



- ✓ 20,000 user capacity
- ✓ Can withstand extreme conditions
- ✓ With Wiegand and OSDP, works with existing access control system
- ✓ Edge solution for fast and accurate recognition
- ✓ High throughput
- ✓ Easy enrollment options
- ✓ Supports dual or single-factor authentication
- ✓ Touchless access to doors
- ✓ Works in extreme lighting conditions indoor/outdoor
- ✓ Get real-time reporting and auditing
- ✓ Grant/revoke access instantly
- ✓ Audio enabled
- ✓ Reader management configuration software

## Typical Wiring



# SAFR SCAN Specifications

Biometrics	
<b>FAR (1:1)</b>	Up to 0.0001%
<b>FAR (1:N)</b>	Up to 0.0001%
<b>Per Device (1:1)</b>	Up to 20,000 Users
<b>Per Device (1:N)</b>	20,000 Users
<b>Match Speed</b>	3 Images per Second
<b>Throughput</b>	60 People per Min

General Electrical	
<b>Power Over Ethernet</b>	PoE IEEE 802.3af, class 3
<b>Power</b>	12VDC @ 1A
<b>Remote Wiring</b>	PoE, OSDP, Wiegand, TTL, Relay
<b>Wiring Connections</b>	OSDP In/Out, Wiegand In/Out, TTL In/Out, Relay

Compliance	
<b>Certifications/Directives</b>	FCC, CE, ROHS
<b>Electromagnetic Immunity</b>	CE (pending)
<b>Security</b>	IEC 62599-1, IEC62599-2
<b>Safety</b>	UL 294, UL 62368-1 Ed. 3 (Outdoor) (Pending)
<b>Environmental</b>	IP65, IK08
<b>Electromagnetic Emissions</b>	FCC

Communication	
<b>Transmission Protocols</b>	IPv4, IPv6, TCP/IP, UDP, DHCP
<b>Compression type</b>	H.264, MJPEG, H.264, H.265
<b>Network Encryption</b>	TLS 1.2 and TLS 1.3 encryption, 802.1x port based authentication
<b>Video Outputs</b>	RTSP
<b>Administrators</b>	Up to 10
<b>Network</b>	10/100MB
<b>Tamper</b>	Inertial measurement unit (IMU) Accelerometer

Audio	
<b>Speaker</b>	1.2W 86dB IP67
<b>Microphone</b>	Omnidirectional
<b>Streaming</b>	2-way, full duplex
<b>Compression</b>	G.711, 8 kHz
<b>Protocol</b>	SIP

Mechanical	
<b>Dimensions</b>	5.5" x 5.5" x 1.25"
<b>Display Dimensions</b>	3.5" color capacitive touch
<b>Color</b>	Black
<b>Material</b>	Aluminum, chemically strengthened glass
<b>Weight</b>	16 ounces
<b>Light Source</b>	IR and LED internal
<b>Operational Distance</b>	0.3 to 1.2M

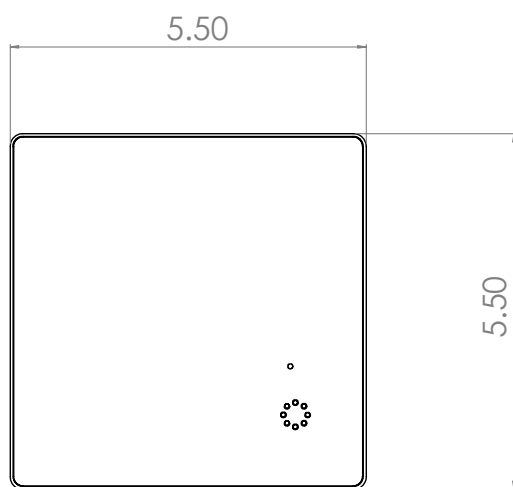
Access Control Requirements	
<b>Input/Output</b>	2 programmable I/O, Form C relay
<b>Protocols</b>	Wiegand in/out, OSDP in/out
<b>RF technology</b>	NFC, ISO 14443, ISO 15693, Mifare, DESfire, EV1, EV2, HID iClass, Elite, SeOS, BLE, UWB, SFR-SC200-RF
<b>Card formats</b>	26-bit, 34-Bit, 35-Bit, 37-Bit, Custom up to 254 Bits
<b>Supports unlock through:</b>	(Face/ID card/Pin/)
<b>Supports authentication with mask</b>	Yes
<b>Recommended Mounting Height</b>	46 to 58 inches
<b>Liveness (anti-spoofing)</b>	RGB, 3D structured light
<b>QR Code</b>	2 dimensional bar codes

Environmental	
<b>Operating Temp</b>	-20C (-4F) to +50C (+122F)
<b>Humidity</b>	0% to 90% (non condensing)
<b>Storage Temp</b>	-40C (-40F) to +60C (140F)

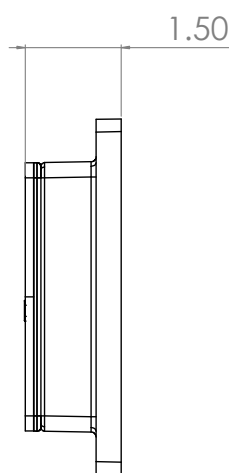
# SAFR SCAN Specifications (continued)

Part Numbers	
<b>SFR-SC100</b>	Facial Recognition Indoor/Outdoor Station, RGBIR Sensor, Face Priority Auto Exposure, 3.5" Capacitive Touch Screen, IR LED, White LED, Wiegand, OSDP, I/O, Audio Full Duplex, PoE/12V DC
<b>SFR-SC200-RF</b>	Facial Recognition Indoor/Outdoor Station, RFID 26, 34, 35, 37-Bit, Custom up to 254 Bits, RGBIR Sensor, Face Priority Auto Exposure, 3.5" Capacitive Touch Screen, IR LED, White LED, Wiegand, OSDP, I/O, Audio Full Duplex, PoE/12V DC
<b>SFR-SCWDG-45</b>	Wedge, 45 degree mount
<b>SFR-SCFMA-100</b>	Flush Mount Adapter

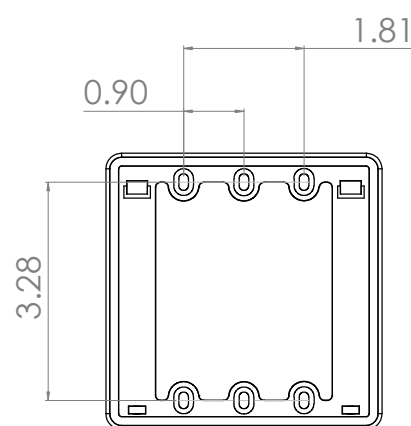
**Front**



**Side**



**Mounting Plate**



Contact [sales@1pcsc.com](mailto:sales@1pcsc.com) for pricing and availability



**Get the SAFR Key App**



# **RealNetworks SAFR SCAN Data Security and Privacy**

## **Introduction**

RealNetworks understands that Privacy and Information Security are mission-critical functions in modern organizations. Our customers trust RealNetworks to delivery safe, accurate and secure facial detection and recognition technology deployed on secure tamperproof hardware. That trust requires a solution that is highly secure and delivers the highest data protection.

This document provides an introduction to RealNetworks' approach to security to safeguard user data and how RealNetworks facilitates organizations comply with regulations related to privacy.

## **RealNetworks and Service Security**

### **About RealNetworks**

RealNetworks is the market-leading facial recognition provider that securely implements facial recognition technology to perform age, gender detection, facial detection and facial recognition via the RealNetworks SAFR SCAN access control device.

### **RealNetworks SAFR SCAN**

RealNetworks SAFR SCAN is the face recognition access control device built and maintained by RealNetworks.

RealNetworks also offers software solutions that enhance the capabilities of SAFR SCAN. This document is limited to RealNetworks SAFR SCAN device and its interactions with SAFR Software or to external systems through REST APIs.

RealNetworks SAFR SCAN provides the following key benefits:

- It can be deployed on private networks with no connection to the cloud and no dependencies on external servers.
- It can be deployed in existing access control systems because it leverages open standards such as OSDP and Wiegand.

- It's regularly updated with security enhancements and new features and made available to customers.
- It allows data to remain on-device protected behind secure encrypted firmware and secure boot.

## **SAFR SCAN Application Products**

Application Products are geared toward organizations that require minimal customization. At a very high level, these products simplify the way people deploy SAFR SCAN. The Application Products include:

- **SAFR Server:** A server application that connects securely to one or more SAFR SCAN devices and performs synchronization of persons across devices, aggregation of events and management and configuration of all connected SAFR SCAN devices. This application can be run on-premises which allows the customer to keep all data on site.
- **SAFR Desktop:** A Windows Desktop application that will connect to SAFR Server and provide the user interface for person management, live event view and device configuration.
- **SAFR Mobile:** An iOS or Android Mobile application that will connect to SAFR Server and provide the user interface for person management, live event view and device configuration.
- **SAFR Actions:** Connects to SAFR Server and automates desired actions based on events such as triggering a notification.

All above components can be installed entirely within an organizations network. With the exception of an initial licensing performed either directly or via downloaded keys, no connection to the Internet is required, thus allowing organizations to provide the highest levels of security for the data.

## **SAFR SCAN API Products**

API Products are provided to enable partners to integrate to external processes and applications to implement same capabilities available with SAFR SCAN Applications. With the API Products, you can:

- **Computer Vision Service API (COVI):** Performs recognition and identity management.
- **Event Service API (CVEV):** Real-time events and event archive access.
- **Video Recognition Gateway (Virga):** Video feed recognition, configuration and monitoring.



- **Object Service API (CVOS)** – Object storage and data stream access.

All of above APIs work directly with the on-premises SAFR Platform installation.

RealNetworks APIs provide programmatic access to the RealNetworks Face Recognition Platform, enabling your developers to build great user experiences or extend RealNetworks solutions.

## **RealNetworks' Approach to Security**

The RealNetworks SAFR SCAN is designed, built, maintained, monitored, and regularly updated with security in mind. The remaining of this document describes how the RealNetworks SAFR SCAN handles data securely and gives organizations control over the data it stores and the lifecycle of that data. Organizations can choose what data to store and how long to store it in order to maintain full compliance with local privacy laws.

### **Data Security (Data-at-Rest Security)**

RealNetworks made multiple investments to ensure customer data is secure and available. Customer data, and access to it, is isolated at the customer premises. Physically, that data is stored on the SAFR SCAN device or the host computer on which the SAFR Server is installed. Data is encrypted at rest (on disk) with AES-256 and RSA-2048 ciphers.

### **Network Security (Data-in-Transit Security)**

Any request to access data must be authenticated using role-based credentials. Requests are made over TLS (https) to encrypt all transactions. An authenticated user's permission is controlled by an access control list (ACL) that independently determines read/write permissions per user role. All access is logged and available for auditing.

### **Device Security (Data-in-process Security)**

SAFR SCAN prevents access to the device firmware by isolating its operation, protecting it from inspection and ensuring that the boot process is secure. The device has a secure boot that prevents rogue OS loading / tampering. Secure boot is backed by mask-programmed boot ROM which acts as a hardware root-of-trust. Initial stages of the boot process are verified via on-chip memory with keys stored in the on-chip One Time Programmable (OTP) area. Signature



verification uses 2048-bit keys and SHA-256. Serial connections, JTAG and USB-boot are not possible because the hardware bridge severed at production. Only access to device is via SSH when explicitly enabled by authenticated user (disabled by default).

## **Personal Data**

Biometric data extraction is performed on personal images input to the system. Biometric data matching is performed against biometric data stored within the system for the purpose of identification. Gender and age are extracted based on facial images input into the system. All processing is optional via per-deployment configuration. Biometric data is optionally associated with personal identification such as name, email, phone and alternate id. Below describes the PII data managed by the SAFR Platform:

- Biometric face data - Information extracted from a face. This information cannot be reversed to obtain the face image. It is used to determine if another face image is similar by comparing biometric face data from each image. It is meaningful only within SAFR service. Therefore, on its own it is not personally identifiable data.
  - Biometric face data that is being compared against pre-populated database biometric face data is not persisted. It exists only for a fraction of a second to facilitate comparing against pre-populated database. After comparing is completed the generated biometric data is irreversibly destroyed.
- age - Estimate of the person's age based on an image of a face
- gender - Estimate of a person's gender based on an image of face
- image of cropped face - The cropped image of the face used to generate the biometric data and age and gender estimate. This is used for display purposes. It is optional.
- Organization supplied data – If biometric data is collected, it can be optionally associated with one or more fields of organization provided metadata. This metadata includes standard fields such as name, access credential ID, email, phone and alternate id. This data is entirely optional and managed along with the biometric record.

All PII data referenced above is entirely optional and all recognition functions operate without this data. Biometric face data is required to perform recognition.

## **Object Types**

RealNetworks SAFR manages the following types of objects:

- People – A biometric signature along with an image and optional estimated metadata and organization supplied metadata.
- Events – An action such as face detected or recognized or an action such as access granted. The event may be associated with a person or not have any association to a person (e.g. demographics collection or stranger or unrecognizable face detection). Images can be optionally stored with the event.

Following defines the fields stored for a person and event.

Person Object. All data is optional unless noted.

- Data generated by SAFR
  - SAFR person id (required – Not a global ID. Meaningful only within scope customer-specific SAFR deployment)
  - image of cropped face
  - biometric face data
  - age (can be overwritten by user)
  - gender (can be overwritten by user)
- User Provided data
  - id class (stranger, no-concern, concern or threat)
  - expiration date
  - alternate id
  - name
  - access credentials
  - company
  - email
  - phone
  - person type (e.g. employee, guest)
  - home location
  - tags - user supplied tag field
  - moniker (alternate identifier for 2-factor authentication)

Event Object (all data is optional unless noted)

- event id (required – Not a global ID. Meaningful only within scope customer-specific SAFR deployment)
- event type
- action id

- face image (cropped face from recognition event)
- scene image (image of full video frame from recognition event)
- action type
- age
- sentiment (average, min, max)
- company
- direct gaze duration
- gender
- moniker
- name
- id class
- person id
- person tags
- similarity score
- smile duration
- tag id
- tag type
- person type
- source
- site
- validation email
- validation phone
- home location
- company
- moniker
- start time
- end time

## **Types of Data**

Demographic Data (age, gender) is extracted directly from the face image. At no time is a face signature generated in order to obtain this information.

Demographic data collected can be optionally associated with a biometric signature but is not required. Demographic data is store as part of an event which records the time and metadata associated with an action such as the appearance of a person on camera.

Biometric data generation and collection is optional. If generated, this information in transmitted securely as noted above. If configured to do so, the biometric data may be stored securely on disk in the encrypted database as noted above.

Events may be optionally generated that record appearance on camera or action of an individual. This data is again transmitted securely and stored in encrypted database for a configurable amount of time. Events do not contain any biometric information.

## **Control over Data Collection**

Integrators and customers have complete control over what data is created and/or persisted. Only data required for the required use case need be stored. Use cases that do not require any PII data such as anonymous demographics reporting can be performed without the need to ever create a biometric signature or storage of any personal data. Use cases that do require biometric signature can be performed without every storing images or personal metadata. Controls allow independent application of these rules to known and unknown individuals.

Integrators can carry out data acquisition policy in the following ways:

- Control is provided to determine what information is acquired from video or Image input inputs
- Control over what information is stored for Persons or Events data

Integrators are encouraged to manage data in compliance with applicable regulations.

## **Users' visibility of Data**

All PII data stored is centralized and APIs exist to facilitate read/write access to PII data. System integrators and customers can access all PII data for a person for purposes of giving user visibility into the data stored about that person. This facilitates the PII requirements to allow users to view and manage.

## **Control over Data Retention**

Customers have control over retention. Person records and events can be configured to be persisted based on lifecycle policies (e.g. store visitor data for maximum of 24 hours). Data is then purged based on lifecycle policies applied. Lifecycle policies can be applied at the person level (all data associated with a person) or at the event level (all data associated with a recognition event or other action). Customers are encouraged to manage data in compliance with applicable regulations.

It is also possible for integrators to provide API and application level control over PII data that enables those integrators to delete any PII data on demand. For example, an integrator can easily implement methods to carry out users requests for their data to be deleted. These actions delete all data associated with a person and event data associated with a person.

In summary, integrators can carry out data retention policy in the following ways:

- Persons or Events can be deleted using the SAFR Desktop Application
- Persons or Events can be deleted using SAFR Service APIs
- Persons or Events can be deleted automatically after a configurable time from record creation

Data deletion is immediate and comprehensive. Deletion of a person deletes all metadata and images stored for that person. Deletion of an event deletes all images and metadata associated with the event.

## **RealNetworks' Encryption Architecture**

RealNetworks uses a multi-layer encryption architecture to protect data at rest and over the wire:

The architecture provides encryption in multiple layers:

### **SAFR Encryption**

RealNetworks encrypts the communication between the service and clients using HTTPS with strong encryption algorithms and keys (2048-bit RSA) and allows tenants to customize their experience and bring their unique domains and certificates.

Security Benefits:

- Confidential data is encrypted in transport
- The connection uses strong encryption algorithms such as TLSv1.2 + TLS1.3
- You can bring your own certificates

### **Device encryption**

RealNetworks encrypts the device firmware. The encryption is performed using symmetric encryption 256-bit AES with exclusive keys per device.

#### Security Benefits:

- Secures device firmware from inspection
- Database exclusive symmetric keys ensures device segregation

#### **Tenant data at rest**

RealNetworks encrypts the tenant confidential data in the database. The encryption is performed using symmetric encryption 256-bit AES with exclusive keys per database.

#### Security Benefits:

- Confidential data is encrypted
- Signs and encrypts SAML and WS-Federation assertions using strong keys
- Database exclusive symmetric keys ensures data segregation

If images are optionally stored, they are stored separate from biometric information and separate from person record. The images are encrypted with exclusive per tenant keys.

#### **Tenant keys at rest**

All the tenant-deployed exclusive keys are stored in a tenant exclusive keystore. The keystore can be accessed only with a tenant-exclusive master key. The unique tenant keystore and tenant exclusive keys mitigates damage if a single tenant is compromised.

#### Security Benefits:

- RealNetworks segregates not only the data and assertions, but also the keys used by tenant
- Tenant keys are only cached in memory for a short time and never stored on disk

#### **Keystore storage and segregation**

The tenant-exclusive keystores and their respective master keys are stored in different locations.

## Security Benefits:

- The storage separation helps protect the keystore confidentiality

## **Data Access Controls**

SAFR has mechanisms in place to delegate accountability of PII data.

User Roles and Permissions control makes it possible to restrict access to data to only those personnel that are authorized. Permissions allow independent read/write control over the data and roles enable grouping of individuals given access to the system to ensure consistency in access granted to the data.

## **Service Logging and Auditing**

Service logs track all actions by user. Any action taken by a user is thus recorded and available for auditing. Information about the action taken, the data to which it was taken (using anonymous IDs), the time and the user taking that action is recorded. Logs are centralized to a single location to facilitate integration to a log collection and auditing service.

## **Service Configuration Security**

Application configuration files are centralized to a single location on disk to facilitate application of OS level access controls. The SAFR services are run under a unique user so that access system resources can be limited to just the resources required for SAFR operation.

## **Privacy impact assessment**

RealNetworks recommends customers conduct a privacy impact assessment specifically for your solution/software and perform a DPIA. RealNetworks has in the past supported customers in this effort. RealNetworks has also performed DPIA for SAFR consumer applications.

## **Best Practices**

<https://safr.com/safr-best-practices/>  
<https://safr.com/the-safr-guiding-principles/>



## Conclusion

A critical aspect of data privacy protection are procedures and policies practiced by the organization deploying SAFR Service. While RealNetworks provides all the tools necessary to maintain data security and privacy, it's the responsibility of the organization implementing this technology to act responsibly and legally. To guide organizations in implementing the SAFR technology, we provide documentation on how to use SAFR to manage personal information and publish the [SAFR Guiding Principles](#) on safr.com.

## **SAFR and General Data Protection Law**

The European Union (EU) General Data Protection Regulation 2016/679 commonly known as “**GDPR**” is designed to provide extensive protection to personal data of individuals located in the EU.

“**Personal data**” is defined broadly as any information relating to an identified or identifiable individual. Videos, still images, cropped faces and biometric signatures captured or generated by SAFR will all be considered personal data under GDPR.

GDPR imposes a number of new obligations on both “**Controllers**” (companies that decide why and how personal data are processed) and “**Processors**” (companies that assist controller to handle personal data). The primary responsibility lies with the Controller, but the Processor is also subject to a number of specific obligations.

In the context of SAFR, our Customers will generally act as the Controller given that they decide whether and for what purpose to use our technology.

The purpose of this paper is to help our Customers to comply with their obligations under GDPR in deploying SAFR. It is intended to provide a framework to inform your own legal review of the application and is not meant to be comprehensive nor provide legal advice. The Customer must advise itself of all obligations under GDPR for the processing of personal data.

### **SAFR and Key GDPR Requirements**

When deploying SAFR or any other facial recognition solution, Customer should be mindful of its obligations under GDPR.

#### **(A) Compliance with GDPR Core Principles**


The deployment of a facial recognition solution should comply with the core principles of the GDPR. Of particular relevance in this context are the principle of purpose limitation (i.e. data can only be collected and processed for specified, explicit and legitimate purposes) and data minimization (i.e. data must be adequate, relevant and limited to what is necessary in relation to the purposes).

## (B) Notice

Any customer who seeks to collect personal data should provide adequate notice to the individuals concerned. While the required notice will depend on the context, consider at minimum placing a sign with the key information in a location visible to all individuals prior to entering the premises.

A model proposed by the EU body in charge of interpreting the GDPR is copied below by way of illustration:

Example:




**Video surveillance!**

Identity of the controller and, where applicable, of the controller's representative:

Contact details of the data protection officer (where applicable):

Purposes of the processing for which the personal data are intended as well as the legal basis for the processing:



Further information is available:

- via notice
- at our reception/ customer information/ register
- via internet (URL)...

**Data subjects rights:** As a data subject you have several rights against the controller, in particular the right to request from the controller access to or erasure of your personal data.

For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.

A detailed notice containing all information required under the GDPR should be accessible on premise in paper format or online, e.g. via a QR-code on the sign.

## (C) Legal Basis for processing (Special Categories of) Personal Data

Any collection of personal data should rely on a justification taken from an exhaustive list of possible justifications included in the GDPR, known as the “legal basis” for processing of personal data. The justifications on which the Customer can rely will depend in particular on whether ‘special categories’ of personal data are processed (one such special category being biometric data).

For SAFR, this is linked to the type of deployment. SAFR deployment can indeed be categorized into two types, namely:

- (a) SAFR for Analytics<sup>1</sup>
- (b) SAFR for Watch-list<sup>2</sup>

### SAFR for Analytics

SAFR for Analytics provides analytical data relating to a data source, primarily a video feed. In this implementation SAFR analyses the images captured from the video feed and provides demographic data such as gender, age, and sentiments. At no time a face signature is generated in order to obtain this information. Demographic data is stored as part of an event which records the time and metadata associated with an action, e.g. the appearance of a person on camera.

Given that SAFR analytics only uses the photo and demographic data generated on that basis (no biometric information), SAFR for Analytics can be implemented by relying one of the justification specified in Article 6 of GDPR. Some of those justifications are as follows:

1. Consent from the imaged individual
2. Legitimate Interest of Customer or a third party
3. Need to Comply with legal obligations of Customer

### SAFR for Watch-list

SAFR for Watch-list allows Customer to pre-load images of a watch list to the SAFR database and uses that database to specifically identify individuals from a video feed. When the customer pre-loads the images to the database, SAFR creates a unique identifying signature for each individual in the watch-list (biometric data), and stores the signatures for cross reference purposes. Each signature is unique to SAFR and cannot be used outside the SAFR product.

---

<sup>1</sup> SAFR for Analytics covers both analytics and security purposes where the biometric information is not processed. Examples include people counting, gender and age recognition, objection recognition (such as firearms) or pet recognition.

<sup>2</sup> SAFR for Watch list covers all implementations where the biometric signature is processed. Examples include security watch-list, secure access and unique people counting.

When deployed SAFR takes a snapshot of the face of each individual in the video feed, creates a biometric signature from such snapshot, and cross references such signature with the signatures in the database. If there is a positive match, event logs will be created of that event along with the picture taken at the time of such collection.

Given that SAFR processes biometric information in this implementation, the Customer will need to rely on a combination of one of the justifications from Article 6 (see above) and one of the justifications from Article 9. Some of the justifications for processing of special categories of personal data are as follows:

1. Explicit consent from the imaged individual
2. Necessity of the processing for the establishment, exercise or defense of legal claims
3. Processing limited to personal data which are manifestly made public by the data subject
4. Existence of a substantial public interest, on the basis of EU or Member State law.

For this second type of processing, it is in addition advisable for the customer to carry out a data protection impact assessment (“**DPIA**”) before processing any biometric data. GDPR recommends a DPIA when the processing involves new technologies that may result in a high risk to the rights and freedoms of the individuals whose data are processed. Also DPIAs are mandatory in the case of automated processing, large-scale processing, or when Controllers systematically monitor a publicly accessible area on a large scale. When the DPIA indicates that processing is likely to result in a high risk to individuals and the Controller is not in a position to take sufficient measures to mitigate such risk, it may also have to consult the competent data protection authority.

Practically speaking, given the nature of the SAFR technology and the type of use cases, it is always advisable to prepare a DPIA prior to the deployment of SAFR for Watch List to understand the risks and the options to mitigate those risks.

#### *(D) Maintaining Control over Processing Activities*

GDPR not only regulates the collection of data, but it also regulates the processing of data. The individuals whose data is collected have rights over such

data, the Controller has obligations towards the individuals and the Processor has certain obligations towards the Controller relating to, among others, security and data management.

SAFR tools provide Customers with complete control over the collection and use of data to assist Customers in complying with their obligations under GDPR. Following are some of the examples of the requirements from the GDPR and the tools available in SAFR for the Customer to control and manage data.

<i>GDPR Obligation (non-exhaustive)</i>	<i>SAFR Tool/ Feature</i>
Data minimization obligation (i.e. the obligation to collect only data necessary for the purpose)	“Person Object” and “Event Object” tools allow the customer to control collection of individual data types. While certain implementations require collection of certain types of data, for example in watch-list SAFR must collect the biometric signature but all other data collection is optional and can be turned off by the controller. (see Annex A for further details)
Rights of individuals to obtain access to their data and the deletion thereof under certain circumstances	The above mentioned tools also give the ability for the controller to access stored data and delete or otherwise manage the data of individuals.
Storage limitation obligation	Timestamps can be set at people or event level, allowing to implement a retention policy with regular deletion of events after a predetermined time period.
Data integrity and confidentiality obligations (taking the necessary technical and operational security measures)	All data is encrypted at rest using AES 256 standard, and the biometric signatures and the photos are stored separately. Administrator access controls are also provided for accessing the system and its data.

Data integrity and confidentiality obligations (backup and restoration of data & audit trail)	<p>Backups occur daily and old backups are destroyed automatically. Backup retention is configurable by the client.</p> <p>Logs are maintained and processed through log analysis tools. Retention thereof can be configured through the tools provided.</p>
---	--

(E) Relationship between Customer and RealNetworks under GDPR

***SAFR Local and SAFR Cloud***

*SAFR Local*

SAFR is offered primarily as an on premises solution deployed on private networks with no connection to the cloud, except for initial licensing requirements and maintenance. With SAFR Local, Customer has complete control of the data through the tools described above. SAFR team provides continuous support by updates and patches to keep SAFR secure from third party vulnerabilities.

*SAFR Cloud*

SAFR Cloud solution offers an opportunity for Customer to use SAFR Cloud Services to process data. In this deployment the data collection will be managed and controlled by Customer using the local client, and RealNetworks will process data in RealNetworks' cloud environment hosted at Amazon Web Services (AWS) in the United States.

As mentioned above, in this cloud solution, Customer will be considered the Controller for GDPR purposes and RealNetworks will be considered Processor.

*Technical and organizational measures for processing*

Under GDPR Controller (Customer) should only use Processors that can provide sufficient guarantees that they have implemented appropriate technical and organizational measures to ensure that processing will meet the integrity and confidentiality requirements of GDPR.



RealNetworks process data in its servers located in AWS. Similar to the local deployment Customer will have complete control over data, which is segregated by each customer and user directory. All data is encrypted at rest with AES-256 and RSA-2048 ciphers. Any request to access data must be authenticated using role-based credentials and requests are made over TLS (https) to encrypt all transactions. Data is stored encrypted and decrypted only on request by authenticated clients. An authenticated user's permission is controlled by an access control list (ACL) that independently determines read/write permissions per user role. All access requests are logged and available for auditing. Further information can be provided upon request.

### *Data Processing Agreement*

Under GDPR, Controllers who call on a Processor to process personal data on their behalf and upon their instructions also need to execute a data processing agreement with the Processor, containing a set of mandatory provisions imposed by the GDPR. The purpose of this agreement is to ensure that the Processor complies with the obligations of Processors under GDPR and that the Processor provides the Controller with the assistance required to enable the latter to comply with its own GDPR obligations.

RealNetworks will enter into such contract for Cloud Deployment.

### *Exhibit A – List of data that can be collected by SAFR and individually managed*

	<b><i>Description</i></b>
	Person Object. All data is optional unless noted <ul style="list-style-type: none"><li>• Data generated by SAFR<ul style="list-style-type: none"><li>• SAFR person id (required – Not a global ID. Meaningful only within</li></ul></li></ul>

	<p>scope customer-specific SAFR deployment)</p> <ul style="list-style-type: none"> <li>• image of cropped face</li> <li>• biometric face data</li> <li>• age (can be overwritten by user)</li> <li>• gender (can be overwritten by user)</li> </ul> <ul style="list-style-type: none"> <li>• User Provided data <ul style="list-style-type: none"> <li>• id class (stranger, no-concern, concern or threat)</li> <li>• expiration date</li> <li>• alternate id</li> <li>• name</li> <li>• company</li> <li>• email</li> <li>• phone</li> <li>• person type (e.g. employee, guest)</li> <li>• home location</li> <li>• tags - user supplied tag field</li> <li>• moniker (alternate identifier for 2-factor authentication)</li> </ul> </li> </ul>
	<p>Event Object (all data is optional unless noted)</p> <ul style="list-style-type: none"> <li>• event id (required – Not a global ID. Meaningful only within scope customer-specific SAFR deployment)</li> <li>• event type</li> <li>• action id</li> <li>• face image (cropped face from recognition event)</li> <li>• scene image (image of full video frame from recognition event)</li> <li>• action type</li> <li>• age</li> <li>• sentiment (average, min, max)</li> <li>• company</li> <li>• direct gaze duration</li> <li>• gender</li> <li>• moniker</li> <li>• name</li> </ul>

	<ul style="list-style-type: none"><li>• id class</li><li>• person id</li><li>• person tags</li><li>• similarity score</li><li>• smile duration</li><li>• tag id</li><li>• tag type</li><li>• person type</li><li>• source</li><li>• site</li><li>• validation email</li><li>• validation phone</li><li>• home location</li><li>• company</li><li>• moniker</li><li>• start time</li><li>• end time</li></ul>
--	--