MORPHEAN

EYES WIDE OPEN ON

Privacy Policy

July 2022

Morphean SA, Rte du Jura 37A, 1700 Fribourg, Switzerland
Phone: +41 26 422 00 90 / E-Mail: info@morphean.com
/ Web: www.morphean.com

1 PRIVACY POLICY

Effective date: 1st July, 2022

Morphean SA with registered office, route du Jura 37A, 1700 Fribourg, Switzerland (hereinafter: “us”, “we”, or “our”) operates the **Morphean** Platform (the “Platform”) and the Video Protector Mobile application.

This page informs the User of our policies regarding the collection, use, storage, hosting, disclosure, transfer, and deletion of Personal Data when he uses our Platform and about the choices the User has associated with that data. Morphean is committed to protecting the privacy of the collected Personal Data.

We use Personal Data to provide and improve the Platform. By using the Platform, the User agrees to the collection and use of information in accordance with this Policy.

Unless otherwise defined, terms used in this Policy have the same meaning as in our Terms and Conditions. The provisions set forth in this Policy are explained in a simplifying manner in the Privacy Notice. The User can consult the Privacy Notice anytime.

For reasons of legibility, the male form was chosen in this Policy. Nevertheless, it refers to members of both genders.

The applicable law is the Federal Law on data protection.

1.1 DEFINITIONS

PLATFORM

Platform in the Morphean context means the digital place that makes accessible a variety of information to the Morphean product, such as proactive video surveillance as a service, smart access control and business intelligence analysis.

Morphean can access the Platform for maintenance, updates, help desk and monitoring purposes. We never sign-in to a specific account but have only global access to the Platform as an administrator.

USER

The User is the individual using our Platform. A User is a person who has an individual account to sign-in to the Platform.

As a direct customer of the VSP, the User collects the data when one of the video cameras the User sets up with his VSP is recording or if the User has smart access control or other sensors.

VSP

The Video Service Provider sells the Morphean product to the User and installs it for the User. The VSP can sign-in to the Platform as an administrator for the User.

The VSP has to make sure that the User fulfils local regulations, for example, to be allowed to record and use smart access control.

PASSIVE PERSON

A Passive Person is somebody who will be linked to video analytics or business intelligence analytics because he will pass in front of the lens of a camera or other sensors. This person is aware of a video surveillance system being present in the area and consents to it according to the local regulation. A Passive Person is somebody who will never sign-in to the Platform.

Passive Persons in the video you record are not related to any identity on the Platform, nor are they identifiable by the Platform.

ACTIVE PERSON

An Active Person is a person who will never sign-in to the Platform but will detain an account for smart access control to have access to certain areas of a building at certain times.

DATA CONTROLLER

Data Controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. For the purpose of this Policy, the VSP is the Data Controller of the User's data.

DATA PROCESSOR

Data Processor (or Service Provider) means any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller. For the purpose of this Policy, Morphean is to be considered as the Data Processor.

GDPR

The GDPR (General Data Protection Regulation) is a new set of rules for personal data processing operations conducted by organizations on the European Union (EU) residents. The GDPR became enforceable on May 25, 2018. The GDPR is intended to harmonize data protection laws throughout the EU by applying a single data protection law that is binding throughout each member state.

PERSONAL DATA

In the context of this Policy, the reference to "Personal Data" includes User's Data, Usage Data, Tracking Cookies Data, Service Data and Access Data. Not included are Metadata.

1.2 INFORMATION COLLECTION AND USE

We collect different types of data for various purposes with the aim to provide and improve our Platform.

We collect the data needed for the User to access the Platform. We are hosting this data, including the User's video recordings, on a cloud of a third-party provider (see section 1.12). We are processing the video data to provide the User with the needed information.

All actions of the User are tracked and recorded in an audit log. The User can consult the log at any time.

TYPES OF DATA COLLECTED

User's Data

While using our Platform, we may ask the User to provide us with certain personally identifiable information that can be used to contact or identify the User ("User's Data"). Personally identifiable information may include:

- First name and last name
- Email address
- Phone (Optional)
- Permissions

We may use the User's Data to contact him with services and operational information only. No individual person is identified nor identifiable by a third party.

The User's data will not be used for marketing purposes.

No processing is done on User's data. This information is only used as static information for Platform login and usage.

Usage Data

Usage Data is data collected automatically, either generated by the use of the Platform or from the Platform infrastructure itself (for example, the duration of a page visit).

We may also collect information that the User's browser sends whenever the User visits our Platform. This data may include information such as the User's computer's Internet Protocol address (e.g., IP address), browser type, browser version, the pages of our Platform that the User visits, the time and date of his visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When the User accesses the Platform by or through a mobile device, this data may include information such as the type of mobile device the User uses, his mobile device unique ID, the IP address of his mobile device, his mobile operating system, the type of mobile Internet browser he uses, unique device identifiers and other diagnostic data.

Metadata

Metadata is a description or definition of electronic data or data about data. It is also referred to as "Business Intelligence data" and is part of the "Big data". Metadata are only general and aggregated statistics, anonymous and not related to physical or identifiable persons, used for marketing and loss prevention purposes. Often, Metadata can only be accessed in certain viewing modes. Metadata can include descriptive tags and information about when a document (i.e., a video) was created and what it contains (2 people, 1 male ~40y, 1 female ~35y).

Tracking Cookies Data

We use cookies and similar tracking technologies to track the activity on our Platform and hold certain information used to provide a better experience and never for marketing purposes.

Cookies are files with a small amount of data which may include an anonymous unique identifier. Cookies are sent to the User's browser from a website and stored on his device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Platform.

The User can instruct the browser to refuse all cookies or to indicate when a cookie is being sent. However, if the User does not accept cookies, he may not be able to use some elements of our Platform.

Examples of Cookies we use:

- We use Session Cookies to operate our Platform.
- We use Preference Cookies to remember the User's preferences and various settings.
- We use Security Cookies for security purposes.

Service Data

By running our Platform, depending on the User's personal setup, we may collect various data coming from external sensors installed on the User's sites ("Service Data"). Data collected will come from sensors such as (but not exhaustive) cameras, door controllers, I/O controllers, radars, microphones, speakers, etc…

Data from service processing contains information of passive persons in video records used for live analytics. We potentially save:

- Amount of person entered
- Age range of the person
- Gender of the person
- Time spent at a position or within areas defined
- Transaction done by the Passive Person

The VSP is responsible, in collaboration with the User, to advise clearly the Passive Person about the service. The Passive Person is aware of a video surveillance system being present in the area and consents to it according to the local regulation.

The Service Data is totally anonymous and not related to an identified or identifiable individual person (Metadata, part of the Big Data).

Access Data

Every access of an Active Person on any door is tracked with a result (grant / refused). The time and potentially video footage are saved in an access log.

Access data may include:

- First name and last name
- Credential information (not online identifier)
- Picture of the face (Optional)
- Video footage of access (Optional)

Except agreed otherwise, no subsequent processing is done unrelated to the initial purpose. The access log is stored for 12 months, while video footage is stored for a maximum of 90 days.

We provide a search engine with table results to review access events. The VSP and/or the User has access to it, depending on the setup. The User and his employee must agree to what is done by whom with the VSP.

1.3 Use of Data

We use the collected data for various purposes:

- To provide and maintain our Platform
- To notify the User about changes to our Platform
- To allow the User to participate in interactive features of our Platform when he chooses to do so
- To provide User support
- To gather analysis or valuable information so that we can improve our Platform
- To monitor the usage of our Platform
- To detect, prevent and address technical issues

We do not use Personal Data for marketing purposes.

1.4 Storage of Data

We will store the server logs for 15 days, the Users Audit log for 6 months, and the Users Access Control log for 12 months.

The Users Profile is stored as long as the User is using the Platform.

The Business Intelligence data (Metadata) is stored indefinitely as it is anonymous, not related to any identified or identifiable individual person.

We do not back up video data. The Users video data is retained for a maximum of 90 days, depending on the chosen settings.

1.5 Transfer Of Data

The User's information, including Personal Data, may be transferred to — and maintained on — hosting providers located outside of his state, province, country or other governmental jurisdiction where the data protection laws may differ from those of the User's jurisdiction (see section 1.12).

The User's consent to this Privacy Policy followed by his submission of such information represents his agreement to that transfer.

We will take all steps reasonably necessary to ensure that the Personal Data is treated securely and in accordance with this Privacy Policy and no transfer of Personal Data will take place to an organization or a country unless there are adequate controls in place, including the security of the User's data and other personal information.

1.6 Disclosure Of Data

Business Transaction

If we are involved in a merger, acquisition or asset sale, the Personal Data may be transferred to a third party. We will provide notice before the Personal Data is transferred and becomes subject to a different Privacy Policy.

Disclosure for Law Enforcement

Under certain circumstances, we may be required to disclose Personal Data if required to do so by law or in response to valid requests by public authorities (e.g., a court or a government agency).

1.7 Deletion of Data

a) User

When the User is deleted, all tracked action stays in the system but without relation to an individual person. An ID replaces the Users info. This ID is not anymore related to the User.

b) Passive Person in Video

Automated deletion

A video is stored for a maximum of 90 days (depending on the chosen settings). Thereafter it is automatically deleted.

On-Demand deletion

If a Passive Person requests to be deleted from the system, the VSP can delete the requested video period, unless this goes against the purpose of the system. As soon as the video is deleted, no further data exists about the Passive Person.

c) Passive Person in Business Intelligence

As the Business Intelligence data (Metadata) of a Passive Person are aggregated and not related to physical or identifiable persons, they are not deleted.

d) Active Person

When an Active Person is deleted, his history is kept and still accessible in the access log but not identifiable.

1.8 The User's Rights

We aim to take reasonable steps to allow the User to correct, amend, delete, or limit the use of Personal Data.

Whenever made possible, the User can update the User's Data directly within his account settings section. If the User is unable to change the User's Data, the User may contact us at **privacy@morphean.com** to make the required changes.

The User is entitled to exercise the following rights with Morphean any time:

- To access and receive a copy of the Personal Data
- To rectify any Personal Data that is inaccurate
- To request the deletion of Personal Data

The User has the right to data portability for the information he provides us with. The User can request to obtain a copy of Personal Data in a commonly used electronic format. We may ask the User to verify his identity before responding to such requests.

The User may request to receive his data, including his video data, for the purpose of transporting them to another data processor.

We include a tool to extract video data. This feature allows the User to extract video per period of 4 hours. We do not (yet) provide dynamic anonymization feature to blur or mask people in video but only static mask for pre-defined area.

1.9 The User's Obligations

The User is responsible for his authentication details and the authorization given to his VSP. The User should read and understand his contract with his VSP, the Term of Services, Privacy Policy and Privacy Notice as well as comply with local Law and regulations, in particular data protection, video surveillance and labour law regulation.

The User is responsible for his video footage and the backup of this footage.

1.10 Third-Party Provider

We may employ third party companies and individuals to facilitate our Platform ("Third Party Provider"), to provide the service on our behalf, to perform service-related services or to assist us in analyzing and monitoring how our Platform is used.

These third-parties have access to the Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose. No third-parties are processing the Personal Data of the User.

Morphean may collect statistics on User's activity in order to enhance Platform's performance and enhance user experience in general.

1.11 Legal Basis For Processing The Data

We collect and process data according to the GDPR and the applicable Swiss Data Protection Regulation. The User collects and processes data according to the GDPR and applicable local laws and regulations with regard to Data Protection and Video Recording and Surveillance.

1.12 Hosting Of The Data

The data is hosted with a third-party cloud service. Currently, we are working with GTT Communications, Inc. The hosting provider has no access to Personal Data.

1.13 Links To Other Sites

Our Platform may contain links to other sites that are not operated by us. If the User clicks on a third-party link, he will be directed to that third party's site. We strongly advise the User to review the Privacy Policy of every site the User visits. We have no access to the content, privacy policies or practices of any third-party sites or services. Therefore, we do not assume any responsibility in this regard.

1.14 Changes To This Privacy Policy

We may update our Privacy Policy from time to time. We will notify the User of any changes by posting the new Privacy Policy on this page.

We will let the User know, via email and/or a prominent notice on our Platform, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

The User is advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

1.15 Applicable Law and Jurisdiction

This Policy and the rights and obligations of the parties hereunder shall be constructed, enforced and governed in accordance with substantive Swiss Law without regard to its conflicts of laws principles. In its scope of application, the GDPR has to be respected. Any conflict arising out of or in connection with this Privacy Policy will be subject to an arbitrage, in the swiss arbitrage center: https://www.swissarbitration.org/centre/.
Pior to that, the parties will endeavour to resolve the dispute through mediation.

1.16 Contact Us

If the User has any questions about this Privacy Policy, he may contact us:

- By email: **privacy@morphean.com**
- By visiting this page on our website: www.morphean.com
- By phone (Helpdesk): +41 26 422 00 98
- Morphean SA, Rte du Jura 37A, 1700 Fribourg, Switzerland
- Website: www.morphean.com
- Helpdesk: +41 26 422 00 98
  General: +41 26 422 00 90