

# Product Privacy Sheet

## Genetec ClearID™

This document is a supplement to the Genetec Privacy Policy available at [www.genetec.com/legal/privacy](http://www.genetec.com/legal/privacy) (the “privacy policy”) and applies to the following Genetec product (the “Product”): Genetec ClearID™.

### Overview

As part of your use of the Product, you (either you as an individual, or the legal entity that you represent, as applicable; referred to as “you”, “your” or “yours”), or your users, may upload, receive or generate data. This document outlines what type of data is concerned and to what extent Genetec (also referred to as “we”, “us” or “our”) may access, store, use or otherwise process (referred to as “processing”, “process” or other similar words) your data.

### What type of data will be captured by the Product?

**Device Data from Synergis™:** To function, the Product must be paired with our access control system, Synergis™. More specifically, the Product requires access to the Device Data from Synergis™ to enable you to associate access rights with entry points. For more information on how Synergis™ handles your data, please refer to the Product Privacy Sheet for Genetec Security Center, available at [www.genetec.com/legal/pps-gsc](http://www.genetec.com/legal/pps-gsc).

**Permanent Cardholder Data:** To allow you to configure access rights, the Product will collect data in the profile you create for each access card holder. This includes mandatory fields, comprised of the first name of the individual, as well as the country in which the person is located. The Product also give you the possibility to add more information through many optional fields, such as the last name, phone number, email, national identifier, employee number, and so forth. Permanent cardholder data will not be made available to Genetec as part of your use of the Product.

**Visitor Data :** When you grant access rights to a visitor, data related to the person will be collected, such as the name, email address and the company for which they work. For traceability purposes, the Product will further collect the time at which a visitor arrives and the reason for the visit. You may also add optional information about your visitors, such as a photo, whether they need assistance, whether a confidentiality agreement is in place, etc. Visitor data will not be made available to Genetec as part of your use of the Product.

**Access Rights Data:** While most of the access rights data will be stored in your Synergis™ system and not accessible to the Product, some data pertaining to the access rights you grant through the Product will be stored exclusively in the Product. This includes the activation and expiration date of an access right, the list of employees and visitors that have

access to a certain location, the fact that an extended time is granted and the reasons for which an access is granted. This allows you to always keep a record of the access granted and the information associated with it.

**Usage Data:** Based on users’ public IP address as determined by the internet service provider, the Product captures the time and approximate location of access of each user. The Product further captures standard usage information. We may have access to this data for analytics and regulatory compliance purposes.

### Data ownership, access and retention

You will always remain the owner of your data. You are fully responsible for the content of your data, which includes obtaining all rights, consents, authorizations and other approvals from all relevant third parties which may be necessary for you to make available your data to us as part of your use of the Product, and for us to process your data in accordance with the terms of our privacy policy and this document.

Your data will be stored in our instance of the Microsoft Azure data centers selected out of the list of regions made available by Genetec in relation to the Product. To minimize risk, permanent cardholder data will be stored in the data center closest to the country specified in their profile. If a cardholder travels from one region to the other, only a subset of the information required to grant access will be transferred to the systems of that region. For guests, the relevant visitor data will be stored in the data center closest to the site visited.

Genetec uses modern encryption standards to maintain the privacy and security of your data in the Product, while in transit and at rest. The data may be accessed only by the authorized system administrators (which may include your system integrator) and users with appropriate access privileges, as defined by you. Genetec personnel do not have access to any customer data that resides in the Product. If Genetec agrees to provide support with regards to the Product, our support team will only have access to information that you submit to us as part of your support request or to which you decide to grant us access through the Product. As such, in certain cases, we may ask you to share additional information with us to be able to respond to your request for support.

The Product does not enable you to configure retention periods, and therefore stores all data until it is manually deleted by you.

This document has been last updated on March 10, 2020. The latest version of this document may be found at [www.genetec.com/legal/pps-clearid](http://www.genetec.com/legal/pps-clearid). We invite you to subscribe to the legal notifications in our [Email Subscription Center](#) to, among other things, be notified of any major changes to this document.