Letter of HITRUST Risk-based, 2-year (r2) Certification

November 19, 2025

Glooko AB
Nellickevägen 20
Göteborg, Sweden 412 63

HITRUST has developed the HITRUST CSF, a certifiable security and privacy framework which incorporates information protection requirements based on input from leading organizations. HITRUST identified a subset of the HITRUST CSF requirements that an organization must meet to be HITRUST Risk-based, 2-year (r2) Certified for a defined assessment scope. Glooko AB ("the Organization") has chosen to perform a HITRUST CSF v11.6.0 r2 validated assessment utilizing a HITRUST Authorized External Assessor Organization ("External Assessor").

Scope

The following platforms of the Organization were included within the scope of this assessment ("Scope") which included a review of the referenced facilities and supporting infrastructure for the applicable information protection requirements:

Platform:

- Glooko Core Platform System residing at Amazon Web Services (AWS) sites in EU-Central-1 (Frankfurt), Amazon Web Services sites in EU-West-1 (Ireland) Glooko AB, Glooko AB (Salinity), and Glooko AB (Shresta Marvel Building)

Facilities:

- Amazon Web Services sites in EU-Central -1 (Frankfurt) (Data Center) managed by Amazon Web Services located in Frankfurt, Germany
- Amazon Web Services sites in US-West (California) (Data Center) managed by Amazon Web Services located in California, United States of America
- Glooko AB (Office) located in Vukovar, Croatia
- Glooko AB (Salinity) (Office) located in Gothenburg, Sweden
- Glooko AB (Shresta Marvel Building) (Office) located in Hyderabad, India

Certification

The Organization has met the criteria specified as part of the HITRUST Assurance Program to obtain a HITRUST r2 validated assessment report with certification ("Certification") for the Scope. Certification is awarded based on each domain's average maturity score meeting a minimum score. Within each domain the maturity scores for each requirement statement were validated by an External Assessor and the assessment was subjected to quality assurance procedures performed by HITRUST.

The Certification for the Scope is valid for a period of two years from the date of this letter assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No security events resulting in unauthorized access to the assessed environment or data housed therein, including any data security breaches occurring within or affecting the assessed environment reportable to a federal or state agency by law or regulation

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST r2 certification criteria specified as part of the HITRUST Assurance Program.

Users of this letter can contact HITRUST customer support (*support@hitrustalliance.net)* for questions on using this letter.

The Organization's Assertions

Management of the Organization has provided the following assertions to HITRUST:

- The Organization has acknowledged that, as members of management, they are responsible for the information protection controls implemented as required by the HITRUST.

- The Organization has implemented the information protection controls as described within their assessment.

- The Organization maintains the information security management program via monitoring, review, and periodic re-assessments of the information protection controls.

- The Organization has responded honestly, accurately, and completely to inquiries made throughout the assessment process and certification lifecycle.

- The Organization has provided the External Assessor with accurate and complete records and necessary documentation related to the information protection controls included within the scope of its assessment.

- The Organization has disclosed all design and operating deficiencies in its information protection controls of which is it aware throughout the assessment process, including those where it believes the cost of corrective action may exceed the benefits.

- No events or transactions have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing the report.

- No actual or suspected security events involving the certified environment have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing the report.

- There have been no communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the Scope of this assessment.

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF assessments, and individual practitioners are required to maintain appropriate credentials based upon their role on HITRUST assessments. In HITRUST r2 validated assessments the External Assessor is responsible for:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.

- Performing sufficient procedures to validate the control maturity scores provided by the Organization.

- Meeting all HITRUST Assessment criteria described within the HITRUST Assessment Handbook.

HITRUST Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization and an External Assessor completed this assessment.

HITRUST performed a quality assurance review of this assessment to support that the control maturity scores were consistent with the results of testing performed by the External Assessor.

HITRUST's quality assurance review incorporated a risk-based approach to substantiate the External Assessor's procedures were performed in accordance with the requirements of the HITRUST Assurance Program.

A full HITRUST Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST Assurance Program can be found at the HITRUST website (https://hitrustalliance.net).

Limitations of Assurance

The HITRUST Assurance Program is intended to gather and report information in an efficient and effective manner. The assessment is not a substitute for a comprehensive risk management program but is a critical data point in risk analysis. The assessment should also not be a substitute for management oversight and decision-making but, again, leveraged as a key input.

HITRUST

HITRUST

Enclosures (2):

- Assessment Context
- Scope of Systems in the Assessment

Assessment Context

About the HITRUST r2 Assessment and Certification

The HITRUST r2 assessment provides the highest level of information protection and compliance assurance. It is the most comprehensive and robust HITRUST certification, and can be optionally tailored to include coverage for additional authoritative sources such as HIPAA, the NIST Cybersecurity Framework, and GDPR.

The HITRUST r2 assessment is an evolving, threat-adaptive assessment with an accompanying certification. HITRUST r2 assessments leverage threat intelligence data and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. To do this, HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks using cyber threat intelligence data from leading threat intelligence providers. Therefore, the HITRUST r2 includes controls that exclusively address emerging cyber threats actively being targeted today.

Assessment Approach

An *Authorized HITRUST External Assessor Organization* (the "External Assessor") performed validation procedures to measure the control maturity of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. These validation procedures were designed by the External Assessor based upon the assessment's scope in observance of HITRUST's CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described elsewhere in this report), and (optionally) reperformance of controls.

Each requirement in the HITRUST CSF contains one or more evaluative elements. For example, requirement 0322.09u2Organizational.12, which reads "Media is encrypted when onsite unless physical security can be guaranteed, and always when offsite.", contains the following two evaluative elements: "1. The organization restricts the use of writable, removable media in organizational systems" and "2. The organization restricts the use of personally owned, removable media in organizational systems". The implementation and operation of all evaluative elements associated with applicable HITRUST CSF requirements included in the assessment was evaluated by the External Assessor in reaching an implementation score.

The PRISMA control maturity scoring model utilized on r2 assessments incorporates the following scale. The overall score for each HITRUST CSF requirement ranges from 0 to 100 points in quarter increments based directly on the requirement's each maturity level scores.

Implementation Score	Description	Points Awarded
Not compliant- (NC)	Very few if any of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment. Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).	0
Somewhat compliant (SC)	Some of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).	25
Partially compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50
Mostly compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75
Fully compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100

Risk Factors

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, technical, and regulatory risk factors.

Assessment Type	
HITRUST Risk-based, 2-year (r2) Security Assessment	
General Risk Factors	
Do you offer Infrastructure as a Service (IaaS)?	No
Organization Type	Service Provider (Non-IT)
Organizational Risk Factors	

Number of Records that are currently held	Less than 10 Million Records
Technical Risk Factors	
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	No - Glooko does not allow personally-owned devices to connect to scoped Glooko assets.
Is any aspect of the scoped environment hosted on the cloud?	Yes
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	No - Glooko does not send information using courier services, internal mail services, or external mail services.
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	Yes
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - Dial-up connections are not used at Glooko. All connections are digital. No analog modems are used business networks.
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - Electronic signatures are not used.
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - Fax machines are not used. All remote document transfers are completed virtually.
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	No - The in scope environment is not E-Commerce and does not perform any sales transactions.
Is the system(s) accessible from the Internet?	Yes
Number of interfaces to other systems	Fewer than 25
Number of transactions per day	Greater than 85,000
Number of users of the system(s)	Greater than 5,500
Is the system(s) publicly positioned?	No - Glooko in-scope system are not accessible from public locations.
Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	Yes
Does the system(s) transmit or receive data with a third-party?	Yes

Are hardware tokens used as an authentication method within the scoped environment?	No - Hardware tokens are not used as an authentication method within Glooko in-scoped environment.
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - Personnel do not travel to any areas that are deemed significant risk.
Are wireless access points in place at any of the organization's in-scope facilities?	Yes
Compliance Factors (Optional)	

Scope of the Assessment

Company Background

Glooko was founded in 2010 to help patients track and manage their diabetes-related glucose and insulin dosage information using its mobile and web applications. In 2016, Glooko merged with Swedish company Diasend to enhance and build a more modern platform based on the strengths of each other's works in the blood glucose sector. The US headquarters are located in Palo Alto, California. The European headquarters are in Gothenburg, Sweden.

The Glooko Core Platform System empowers the management of diabetes and other chronic conditions by collecting and unlocking the power of data from blood-glucose (BG) meters, continuous glucose monitors (CGMs), insulin pumps, connected insulin pens, wearables, connected scales, blood pressure cuffs, and activity trackers – bringing insights together in one place. Data is easily uploaded – remotely via app or in-clinic, securely shared, and visualized in actionable charts and graphs. This creates a solid foundation enabling collaboration and confident treatment decisions. The platform is compatible with over 95% of diabetes devices along with biometric devices, giving people with diabetes and chronic conditions and their care teams the freedom of choice.

The Glooko Core Platform's key functions are:

- Diabetes dosage, tracking, and management for consumers via the web portal and mobile application
- Diabetes treatment management for providers via the web portal
- Third-party partner integration for diabetes treatment and management via the Application Programming Interface (API)

In-scope Platform

The following table describes the platform that was included in the scope of this assessment.

Glooko Core Platform System	
Description	Glooko Core Platform System utilizes AWS to host the application servers, database servers, and supporting services. The web application is served through a redundant AWS Elastic Load Balancer connected to several AWS Elastic Compute Cloud (EC2) instances that host the application servers. These environments connect to several components, which complete the different operations required to process data from diabetes management devices. The data from diabetes management devices like BG meters, CGMs, and insulin pumps are uploaded to Glooko Core Platform by transmitters, uploaders, or mobile apps. Once connected to the AWS Load Balancer through HTTPS/SSL, data reaches one of the AWS EC2 instances in the VPC, which securely connects to the database to retrieve or add data. The data is then parsed by Analyzer, which then talks to the backend APIs and updates the data in the database. The data is then visualized in the web interface in the Summary, Logbook, Graphs, and Device settings. Mobile applications are out of scope for this assessment.
Application(s)	Glooko
Database Type(s)	Mongo DB, Snowflake
Operating System(s)	Linux
Residing Facilities	Amazon Web Services sites in US-East (N. Virginia), Amazon Web Services sites in US-West (California), Glooko AB, Glooko AB (Salinity), Glooko AB (Shresta Marvel Building)
Exclusions	Mobile applications

In-scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Amazon Web Services sites in EU-Central-1 (Frankfurt)	Data Center	Yes	Amazon Web Services	-	Frankfurt	Germany
Amazon Web Services sites in EU-West-1 (Ireland)	Data Center	Yes	Amazon Web Services	-	Dublin	Ireland
Glooko AB (Shresta Marvel Building)	Office	No	-	Hyderabad	-	India
Glooko AB	Office	No	-	Vukovar	-	Croatia
Glooko AB (Salinity)	Office	No	-	Gothenburg	-	Sweden

Services Outsourced

The following table presents the outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this r2 assessment. HITRUST requires the inclusive method must be used on HITRUST r2 validated assessments. Under the Inclusive method, HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the External Assessor.

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Amazon Web Services	They provide infrastructure, communication and information storage along with tools for audit logging, monitoring and provide maintenance to all infrastructure services. Following service are being utilized: Amazon Dynamo, AWS VPC, Application Servers, Database Servers, Amazon Lambda, Amazon Security Groups, Amazon Load Balancer, Amazon API Gateway, Amazon Elasticache, Amazon Simple Storage Service.	Included
Jira Atlassian (cloud hosted)	Development Tracking	Included
Papertrail Inc.	Log management	Included
Snowflake Inc.	Data Warehouse	Included