Brilliant Future

Classification: Public

INSIGHT – CX, EX

Architecture, Compliance and Security White Paper

1 DOCUMENT VERSION CONTROL

Rev	Modified	Modified By	Approved By	Document Changes
1.0	2023-01-10, 2023-10-09	Johan Pellbäck	Product management team	New template
2.0	2023-10-09	Johan Pellbäck, Sofie Johansson	Product management team	New sections for CX and AI (chapter 4, 6)
2.1	2024-01-15	Johan Pellbäck	Product Management team	More regarding architecture, SSO etc
2.2	2024-02-02	Johan Pellbäck, Sofie Roos	Product Management team	Complementary chapter 5
2.3	2024-03-20	Johan Pellbäck, Mimmi Lindström	Product Management team, Product Design	Description about design system and WCAG fulfilment
2.4	2024-05-30	Johan Pellbäck, Mimmi Lindström	Product Management team, Product Design	Complimentary info regarding usability and WCAG
2.5	2024-08-12	Johan Pellbäck	Architecture team	Chapter 5. SSO, authentication, tenant model, and data isolation
2.6	2024-11-04	Johan Pellbäck, Jonathan Dahlberg	Architecture team	Chapter 5 as part of WAF implementation using Azure Frontdoor Chapter 7 updates in roles and accountability
2.7	2025-01-08	Johan Pellbäck	Product Management Team	Chapter 5.3 regarding logging
2.8	2025-06-12	Johan Pellbäck	Product Management Team	Chapter 4.1 added features regarding content (communication, questions and surveys)
2.9	2025-06-13	Johan Pellbäck	Product Management Team	Chapter 5.5 added HailyHR as integrated HR-solution Chapter 6 regarding risk with AI
3.0	2025-08-18	Johan Pellbäck, Mimmi Lindström	Product Management Team	Updated section 4.2 regarding compliance with WCAG 2.2
3.1	2025-10-07	Johan Pellbäck	Product Management Team	Updated link to our help center
3.2	2026-04-20	Johan Pellbäck, Mattias Jardstedt	Product Management Team	Updates in chapter 5.5 regarding integrations and APIs. Updates in chapter 7 according to ISO 27001 and SDLC.
3.3	2026-05-20	Johan Pellbäck	Jonathan Dahlberg, Mattias Jardstedt	Updates in chapter 5, describing the implementation of email distribution and security (using SPF, DKIM, DMARC)
4.0	2026-09-23	Johan Pellbäck, Fredrik Kronander, Sofie Johansson	Karl Spjuth, Mattias Jardstedt, Erik Nordenhök	Updates in chapter 4 regarding products/features, chapter 6 regarding architecture, chapter 8 with updates regarding AI, security, privacy etc.
4.1	2026-10-27	Johan Pellbäck	Sofie Johansson	Correction in 4.2 regarding language support

2 DOCUMENT CONTENT PAGE

1 Document Version Control 1
2 Document content page 2
3 Introduction 4
3.1 Purpose 4
3.2 Scope 4
4 Products and features 5
4.1 Products 5
4.2 Languages 5
4.3 Anonymity for Employee surveys (People Intelligence/EX) 6
5 Web Connectivity Accessibility Guidelines (WCAG) 7
5.1.1 General 7
5.1.2 Text Readability 7
5.1.3 Survey 7
5.1.4 Supported Devices 7
5.1.5 Summary 7
6 Architecture 8
6.1 Deployment view 8
6.1.1 Entry point 9
6.1.2 Application services 9
6.1.3 AI components 9
6.1.4 External sub-processors 9
6.1.5 Payment provider 9
6.1.6 Optional integrations 9
6.1.7 Monitoring 10
6.2 Security 10
6.2.1 Securing web application using firewall (WAF) 10
6.2.2 Authentication/SSO, data isolation and tenants 10
6.3 Logging 10
6.3.1 Infrastructure and Security monitoring 10
6.3.2 Application-Level Logging 11
6.3.3 Log retention 11
6.4 Backups 11
6.4.1 Recovery and retention 11

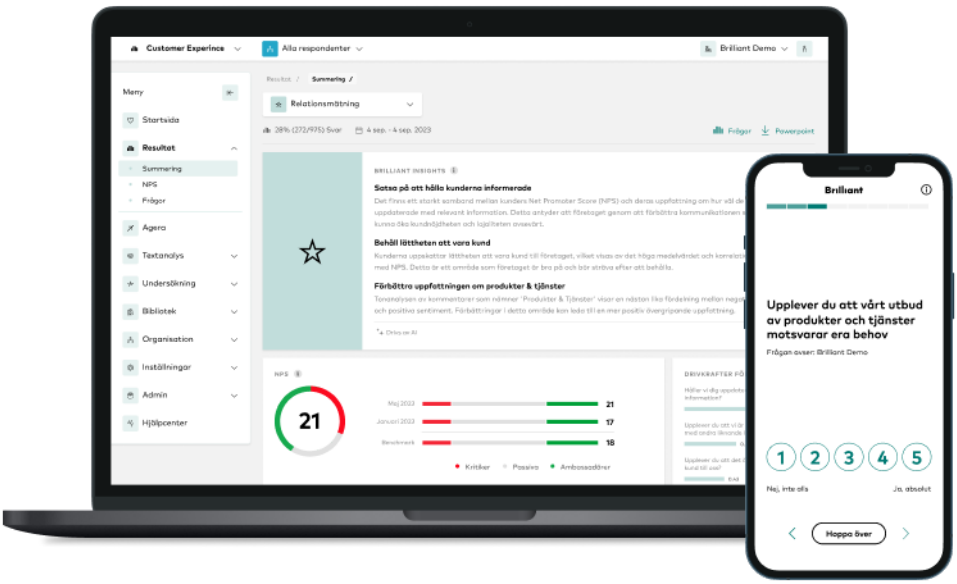
6.5 Integrations 12
6.5.1 3 types of integrations 12
6.5.2 Direct integration 12
6.5.3 SFTP File import 13
6.5.4 Public REST-API 13
6.5.5 Recommendations 14
6.6 Email distribution and security 14
6.6.1 SPF (Sender Policy Framework) 14
6.6.2 DKIM (DomainKeys Identified Mail) 15
6.6.3 DMARC (Domain-based Message Authentication, Reporting and Conformance) 15
7 Data elements and processing 16
7.1 Data transfer and storage 16
7.2 Data elements 16
8 Secrecy, Privacy and AI 17
8.1 AI-supported measurement, insight and actions in beat 17
8.2 Anonymity and data minimisation in Engage and Beat 18
8.3 Team context – Story in beat 18
8.4 Data access and AI output 18
8.5 Risk with the use of AI 19
9 Risks combined with data storage and processing 20
10 Technical and organisational measures 21
10.1 Software development lifecycle process (SDLC) 21
10.2 Roles and responsibilities 21
11 Common questions regarding operations, storing and processing of personal data 23
11.1 References 25

3 INTRODUCTION

3.1 PURPOSE

Brilliant Future is a Swedish SaaS company that helps organisations to reach their full potential through strengthening employee and customer relations. Brilliant's platform is easy to use and built on a well-known methodology that ensures that the entire organisation focuses on the right things. Our solutions improve employee engagement, develop leaders, strengthen employer brand and customer relations.

This document describes our platform Insight, the architecture, technical- and organisational measures implemented for compliance with laws and regulations (such as GDPR and AI-act).



3.2 SCOPE

The Insight application, infrastructure, processes and security measures/controls

4 PRODUCTS AND FEATURES

Insight is Brilliant Future's platform for understanding and improving employee and customer experiences, turning feedback into insight, and insight into action.

Built on more than 25 years of experience, research and our own data, Insight helps organisations understand what drives engagement, experiences and performance. But understanding is only the beginning. The real value comes when insights help people make better decisions, strengthen teams and improve experiences.

Through Engage, Relate and Beat, organisations can collect feedback, uncover patterns and drivers, follow development over time and turn insights into concrete action. HR and senior leaders get the bigger picture and the insights they need to understand where to focus, while managers get relevant insights, recommendations and practical support to develop their teams.

Our ambition is to go beyond surveys, dashboards and reporting. Insight should continuously help organisations understand what is happening, why it matters and what to do next, giving the right people the right support based on their own situation.

Insight supports organisations of different sizes across a global market and is available in more than 40 languages. The SaaS platform provides self-service tools for data management, surveys, analytics, reporting and action across employee and customer experiences.

Because the value isn't in collecting feedback. It's in what you do with it.

4.1 PRODUCTS

This section provides a brief description of the products we offer in Brilliant Insight.

Product	Area	Description
Engage	People Intelligence (EX)	Product for measuring, understanding and acting on the employee experience, using pulse and annual surveys, research-based analysis, AI insights, benchmark and integrated action plans.
Beat	People Intelligence (EX)	Product to support managers and to combine team feedback with manager's own context (Story) to give personal recommendations and concrete activities for building high-performing teams.
Relate	Customer Intelligence (CX)	Product for understanding customers through targeted or recurring surveys, with segmentation, NPS and benchmark, driver analysis, AI text analysis and close-the-loop.

4.2 LANGUAGES

Insight supports multiple languages for both administration and for the survey and can be expanded based on customer needs.

The admin part (for managers, HR, survey admin etc) supports the following languages: Danish, English, Finish, French, Norwegian, Spanish, Swedish, German, Brasilian Portuguese, Estonian, Italian, Japanese, Chinese (Mandarin), Dutch, Polish, Portuguese

More information can be read in our help center: Brilliant Produktbeskrivning EX | Brilliant (brilliantfuture.se)

4.3 Anonymity for Employee surveys (People Intelligence/EX)

Brilliant guarantees that answers are handled confidentially, that answers are anonymous and that answer cannot be derived to individual respondents. A complex set of anonymity rules ensures that the anonymity of the respondents is guaranteed. You can read more about how we guarantee the anonymity in our helpcenter: https://insight.brilliantfuture.se/en/exhelp/anonymity

5 WEB CONNECTIVITY ACCESSIBILITY GUIDELINES (WCAG)

Brilliant Future is dedicated to meeting the accessibility guidelines according to WCAG 2.2 AA. Below is an explanation of how we fulfil these requirements, as well as identified deviations.

5.1.1 General

All graphical elements on our platform meet the required colour contrast and font size standards to be considered accessible under WCAG 2.2 AA.
Deviation: Certain visual graph components provided through Highcharts may lack alternative text or full screen reader support, which can affect users relying on assistive technologies.

5.1.2 Text Readability

All text on our platform is designed to maintain a LIX value (Readability Index) between 40–60 to ensure good readability.
Deviation: Some system texts and error messages may exceed this range, which can make them more difficult to understand.

5.1.3 Survey

Our surveys are developed to meet WCAG 2.2 AA requirements and are designed to support a broad user group. Since customers can apply their own branding, full compliance cannot always be guaranteed. To address this, we provide an option to adjust contrasting colours. Customers may still choose to proceed with non-compliant settings at their own discretion.
Deviation: Minor deviations may occur, but we remain committed to minimising these instances and continuously improving accessibility.

5.1.4 Supported Devices

The platform supports use on desktop, tablet, and mobile devices.
Deviation: The mobile version is optimised for survey participation, while system configuration and management are recommended to be carried out on larger screens.

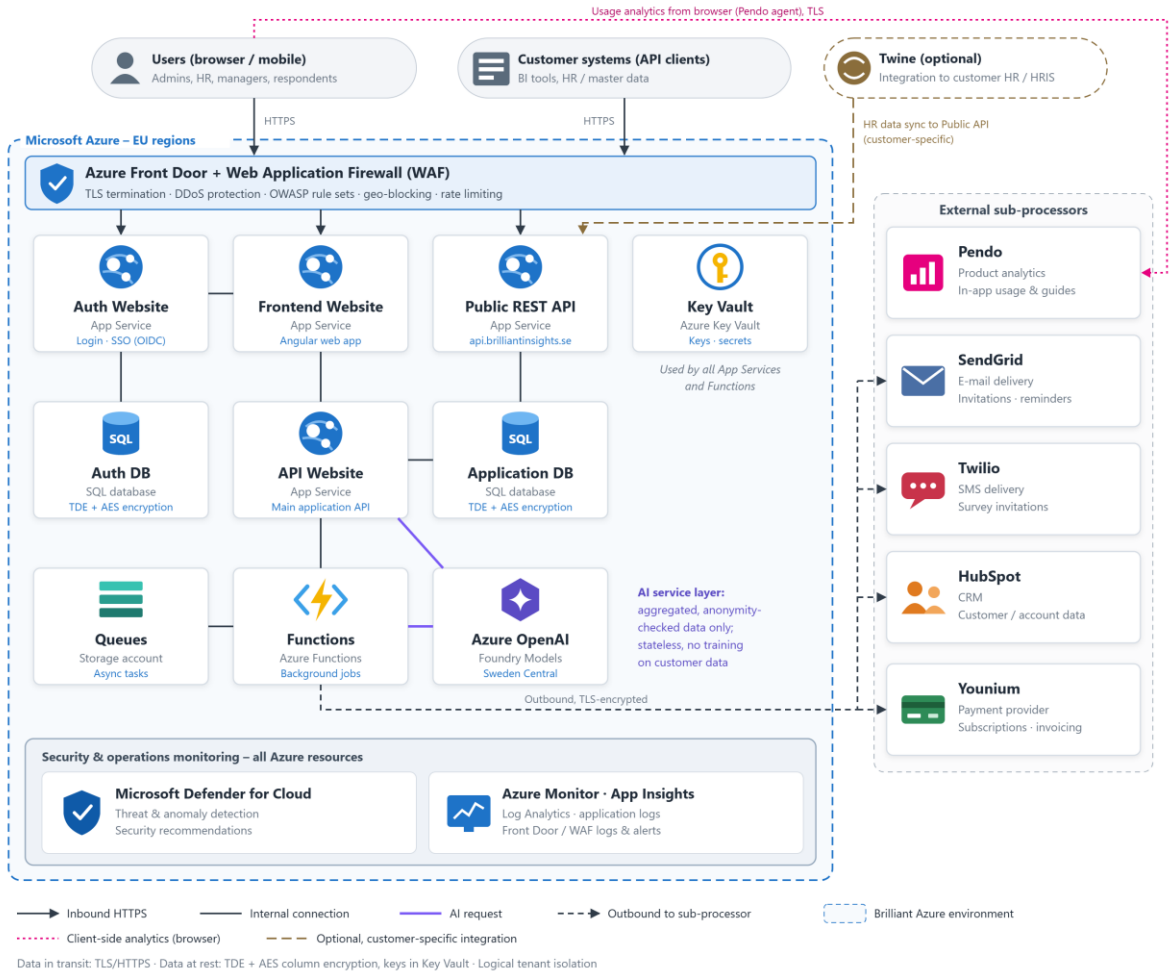
5.1.5 Summary

Brilliant Future is dedicated to fulfilling the requirements of WCAG 2.2 AA. Regular reviews and updates are conducted to ensure the platform remains accessible to all users. We acknowledge the current deviations, primarily related to Highcharts visual graph components, and are actively working to address these and further enhance the user experience for everyone.

6 ARCHITECTURE

The diagram shows the deployment view of Brilliant Insight. All platform components run in Brilliant's Microsoft Azure environment in EU datacenters.

6.1 DEPLOYMENT VIEW



6.1.1 Entry point

All inbound traffic, from end users and from customer systems, passes through Azure Front Door with a Web Application Firewall (WAF). Front Door provides TLS termination, DDoS protection, OWASP rule sets, geo-blocking and rate limiting before any request reaches the application (see 6.2.1).

6.1.2 Application services

The frontend application is an Angular site hosted on an App Service and is the main touchpoint for customers. Credential management, login and SSO integrations (OAuth 2.0 / OIDC) are handled by a separate Auth website. It is hosted in its own App Service with its own database.

The main API, which the frontend communicates with, is hosted in a third App Service. It connects to the main application database and to Azure Functions, which use a storage account with queues for asynchronous and background tasks.

The Public REST API (api.brilliantinsights.se) is hosted in a separate App Service. It gives customer systems access to organisational structure and aggregated survey results, and allows organisational data to be updated (see 6.5).

Both databases are Azure SQL databases with Transparent Data Encryption (TDE). Columns containing personal data are additionally encrypted using AES (see 7.1). All security keys, encryption keys and secrets are managed in Azure Key Vault.

6.1.3 AI components

AI functionality uses Microsoft Azure OpenAI (Microsoft Foundry Models) in the Sweden Central region. It is accessed only through Brilliant's internal application and AI service layer. Only aggregated data that meets Brilliant's anonymity requirements is used, and customer data is not used to train models (see chapter 8).

6.1.4 External sub-processors

The platform uses the following sub-processors, all communicating over TLS-encrypted connections:

SendGrid: email delivery of invitations, reminders and reports (see 6.6)

Twilio: SMS delivery of survey invitations

HubSpot: CRM for customer and account data

Pendo: product analytics and in-app guides. The Pendo agent runs in the user's browser, so usage data is sent directly from the browser to Pendo.

6.1.5 Payment provider

Younium is used for subscription management, billing and invoicing. It does not process personal data on behalf of customers and is therefore not a sub-processor. NOTE! This is used for the Beat-product only.

6.1.6 Optional integrations

For customers who order a direct HR/HRIS integration, Brilliant uses the integration platform Twine. Twine delivers employee and organisational data to Insight through the Public REST API on a scheduled basis (see 6.5).

6.1.7 Monitoring

All Azure resources are continuously monitored by Microsoft Defender for Cloud. Application and infrastructure logs are collected in Azure Monitor, Application Insights and Log Analytics (see 6.3).

6.2 SECURITY

6.2.1 Securing web application using firewall (WAF)

The Insight application uses a web application firewall (WAF) using Front Door for secure entry point for web applications hosted on Microsoft Azure. This provides load balancing, high availability, and global distribution for applications. Azure Front Door also protect the applications from common security threats, such as DDoS attacks, SQL injection, and cross-site scripting, while also supporting SSL termination, end-to-end encryption, and customizable routing rules. With WAF actively blocking known vulnerabilities (e.g., OWASP Top 10), the setup protects the environment against common web application threats. This reduces the likelihood of data breaches or unauthorized access to sensitive information.

6.2.2 Authentication/SSO, data isolation and tenants

SSO: Our Single Sign-On uses multi-tenant model and are designed for security, scalability, and ease of use across our platforms. User authentication is built on top of OAuth 2.0, OIDC designed for authenticating users in modern, web-based applications and mobile apps. Tenant Isolation: Our platform is architected as a multi-tenant system, where each tenant (customer organization) operates in a logically isolated environment. This ensures that each tenant's data remains separate and secure, with robust access controls preventing unauthorized cross-tenant access.

Role based access (RBAC): Within each tenant, we implement fine-grained RBAC to manage user permissions. This allows organizations to define specific roles, such as administrators, analysts, or viewers, to limit access based on the principle of least privilege.

Data isolation: Data for each tenant is logically separated in application as well as in in the database layer. This setup ensures data segregation, preventing data from one tenant from being accessed by users from another tenant.

6.3 LOGGING

Brilliant Insight uses different ways and components for logging, for security and monitoring we use native logging in MS Azure, MS Defender and MS Front door. We also use application-level logging for monitoring security and product related events in the application.

6.3.1 Infrastructure and Security monitoring

Microsoft Defender for Cloud: Insight is continuously monitored using MS Defender, which provides:

- Threat detection for cloud workloads, including VMs, databases, and Kubernetes clusters.
- Anomaly detection for unusual user or system behavior.
- Security recommendations to enhance compliance with Azure security best practices.
- Defender integrates with Azure Sentinel (SIEM) for centralized security analytics and incident response.

Microsoft Azure Front Door: MS Front Door acts as both a Web Application Firewall (WAF) and a DDoS protection layer for Insight. Security capabilities include:

- Rule-based and AI-driven threat detection for SQL injection, XSS, and other web-based attacks.
- Geo-blocking and rate limiting to prevent abuse from suspicious regions.
- DDoS protection against volumetric and application-layer attacks.
- Real-time logging and alerts for malicious activity detected at the network edge (WAF & DDoS Protection)

6.3.2 Application-Level Logging

Insight logs central application events to ensure traceability, incident detection, and forensic capabilities. These logs are stored in the application database or in Azure Monitor / Application Insights / Log Analytics, depending on the log type and use case. The application-level logging relates primarily to the platform, not the survey part.

Authtentication and Access Control: refer to login events, authorization and role management, such as:

- Successful and failed login attempts (including client information such as IP-addresses, and device information)
- Authorization and Role changes (changes to users, roles, permission)
- Modifications to organizational structures and hierarchy

6.3.3 Log retention

All logs are aggregated and stored centrally and securely. Access to logs is restricted based on least privilege principles and is audited regularly. Logs related to infrastructure and security uses standard mechanisms and policies accordance with GDPR and ISO 27001. Application and product level logging follow the same principles as for all our products, e.g. regarding anonymity and encryption. Retention for application level logging follow the customer licensing period.

6.4 BACKUPS

Insight uses automated backup policy specified in Azure SQL Database.

- Full backups every week
- Differential backups every 12 – 24 hours
- Transaction log backup approximately every 10 minutes

6.4.1 Recovery and retention

Azure SQL Database store backup in a geo-redundant environment, meaning that data is replicated to a paired region in case of a regional outage.

The retention policy follow Microsofts recommendation:

- A quick point in time recovery can be done for up to 7 days
- Weekly backups are saved for 2 months.
- Monthly backups are saved for 6 months.
- A yearly backup is saved for 2 years.

6.5 INTEGRATIONS

The most important thing for a successful implementation of Insight, regardless of whether it concerns customer- or employee surveys, is to be able to reflect your organisational structure in a way the meet your need for reporting and analysis.

Brilliant Insight integrates with external systems to keep your organizational data up to date and to allow you to build on top of your engagement data. All integrations are automated — once configured, they run without manual involvement.

6.5.1 3 types of integrations

Type	How	Example
Direct integration	HR system => Brilliant Insight	Insight uses a integration platform from Twine to connect directly to your HR system's and syncs data on a schedule. Twine support multiple direct integrations, read more about Twine here: https://www.twine.se/integrationer
SFTP File import	HR system => SFTP => Brilliant Insight	Your HR system exports a file to a secure SFTP server, Insight picks it up automatically
Public REST-API	Insight <=> Your system	You build your integration directly to us: • Pull engagement data (surveys, results, groups) from Insight into your own tools/BI/master data • Push employee data and update your organizational data directly

6.5.2 Direct integration

A direct integration means Insight connects to your HR system's API and automatically fetches employee and organizational data on a configured schedule.

How it works:

- Insight calls your HR system's API on a schedule (e.g., daily)
- Employee data, departments, and manager relationships are fetched
- Fields are mapped, using Twine integration platform, to Insight attributes (using standard or custom mapping)
- Organization rules run automatically to rebuild the group structure

What gets synced:

- Employee data — name, email, phone, birth date, hire date, gender, active status
- Organization structure — departments, locations, teams, legal entities
- Relationships — manager-employee links
- Custom fields — any additional fields your HR system provides

Custom field mapping: You can configure exactly which fields from the HR system map to which attributes in Insight. This includes standard fields (name, email, department) and custom/company-specific fields. Each mapping specifies a source field, a target attribute, and a data type (user, group, or group relation).

Current support:

Read more about Twine integrations here: https://www.twine.se/integrationer

6.5.3 SFTP File import

An SFTP integration is a fully automated, file-based integration. Your HR system exports a data file to a secure SFTP server on a schedule, and Insight picks it up automatically — no manual steps involved.

How it works:

- Your HR system runs a scheduled export job (e.g., nightly)
- The job writes a CSV/delimited file to Insight's SFTP server
- Insight picks up the file on its own schedule
- The file is parsed using configured column mapping
- Employee and organizational data is imported
- Organization rules run automatically to rebuild the group structure

Configuration:

- SFTP server address, folder, and credentials (provided by Brilliant)
- Column definitions — which columns in the file map to which Insight attributes

This is a true integration, not a manual process. Once the scheduled export is configured in your HR system, data flows automatically without any human involvement.

See our helpcenter for a complete list of HR-systems that support automatic export of employee data: https://insight.brilliantfuture.se/en/exhelp/integration-overview

6.5.4 Public REST-API

The Public API is an integration for reading engagement data out of Insight as well as updating the organizational structure directly. Unlike the HR integrations (which bring data in), the REST-API also lets you pull survey results, group structures, and engagement metrics into your own systems.

Common use cases:

- Display engagement data in BI dashboards (Power BI, Tableau, Looker)
- Build custom reports and exports
- Automate engagement monitoring and alerts
- Correlate engagement data with other business metrics

What you can access:

- Organization structure (groups and categories)
- Surveys and their status
- Aggregated survey results per group, index, and question
- Indexes and questions with localized names

6.5.5 Recommendations

Before starting direct integrations of organisational data, it's important to make sure that the source system can reflect the way results shall be presented and analysed. And that clear processes for managing the organisational structure are in place.

Things to consider:

- Team size – for employee surveys you might want to merge teams to avoid anonymity limitations in the results. Read more about anonymity in our help center: https://insight.brilliantfuture.se/en/exhelp/anonymity
- Primary/Secondary hierarchy – a powerful way of presenting different dimension of the result is to use primary/secondary organisational structure. This can be created using customer specific attributes. This needs to be reflected in the customer data using import files or direct integration.
- Background variables – consider if you want to use background variables and if these should be part of the survey or already in organisational data. Read more about background variables vs background questions in our help center: Bakground variables vs. background questions – Brilliant Helpcenter (brilliantinsights.se)

6.6 EMAIL DISTRIBUTION AND SECURITY

Insight uses email as one of the primary communication channels for survey invitations, reminders, notifications and reporting. To ensure scalability, reliability and secure delivery of outbound email communication, Brilliant uses SendGrid as a sub-processor and cloud-based email delivery platform.

The email architecture is designed to support high-volume transactional communication while maintaining security, authenticity and deliverability. Email messages generated by the Insight platform are transmitted securely to SendGrid through encrypted communication channels using TLS. SendGrid acts only as an outbound delivery service and processes email data according to contractual obligations and Brilliant's sub-processor management process.

The integration with SendGrid provides:

- Scalable delivery of survey invitations and reminders
- Delivery monitoring and bounce handling
- Retry mechanisms for temporary delivery failures
- Analytics related to communication status and delivery outcomes
- High availability and operational resilience for outbound email communication

To strengthen authenticity and protect recipients from email spoofing, phishing attempts and domain impersonation, Brilliant has implemented standard email authentication mechanisms for outbound survey communication:

6.6.1 SPF (Sender Policy Framework)

SPF is configured to explicitly define which mail servers are authorized to send email on behalf of the @brilliantinsights domain. Recipient mail systems can validate that messages originate from approved infrastructure and reject unauthorized sources.

6.6.2 DKIM (DomainKeys Identified Mail)

DKIM provides cryptographic signing of outbound email messages. Each email receives a digital signature associated with @brilliantinsights domain, allowing recipient systems to verify message authenticity and ensure that message content has not been modified during transmission.

6.6.3 DMARC (Domain-based Message Authentication, Reporting and Conformance)

DMARC builds upon SPF and DKIM by defining policies for how recipient systems should handle messages that fail authentication checks. DMARC also provides reporting mechanisms that improve visibility into unauthorized use of domains and attempted spoofing activities.

Together, SPF, DKIM and DMARC provide layered protection that improves email deliverability, reduce risk of phishing and spoofing as well as protecting integrity and authenticity of survey communication.

7 DATA ELEMENTS AND PROCESSING

Security and data integrity are of outmost importance to us at Brilliant Future. This section describes how we store data and additional security measures applied.

7.1 DATA TRANSFER AND STORAGE

The Insight application is hosted as a SaaS-application in Microsoft Azure. The underlying services (web apps, SQL server, Azure functions, Azure vaults) store data using resource groups in datacenters located in West Europe (Netherlands), Sweden Central (Gävle/Sandviken/Staffanstorp), West Europe (Holland).

To further strengthen data integrity, we use following methods:

- **Data in transit** uses standard SSL/TLS/HTTPs with certificates stored separately using App Service Certificate in Azure
- **Data at rest** using SQL server and standard TDE encryption. Columns containing personal data in DB are using AES encryption. Encryption keys are stored separately using Azure Vaults.
- **Anonymization and pseudonymization** of respondents. For employee surveys (EX) it is of outmost importance that respondents are handled with full integrity so that answers cannot be derived to physical person. For EX all answers from respondents are anonymized in the UI and we use pseudonymization when storing data to the database. For customer surveys individuals are not anonymous in the UI, but data is still pseudonymized when stored to the database (data at rest).

7.2 DATA ELEMENTS

Below is a list of personal data stored in Insight and methods associated with securing data integrity.

Element	Purpose	Comment
FirstName, LastName, Email	Respondent information, roles managing organizations, surveys, etc	Encrypted using AES
UserParameters	Additional respondent information (e.g., background information, startdate, age, etc)	Anonymised
UserCredentials	For specific roles with access to Insight we store credentials separately with references to encrypted usersIDs	Anonymised

8 SECRECY, PRIVACY AND AI

For Brilliant Future, privacy, information security and individual integrity are fundamental principles in the use of Artificial Intelligence.

Brilliant uses Microsoft Azure OpenAI / Microsoft Foundry Models within Brilliant's existing Microsoft Azure environment. The Azure AI resources used by Brilliant are located in the Sweden Central region. Different AI models may be used depending on the task.

All AI functionality is accessed through Brilliant's internal application and AI service layer. The application determines the purpose and context of each request and provides only the information required for that specific operation. AI models do not have general access to Brilliant's databases or customer data.

Brilliant does not fine-tune AI models using customer or respondent data. Instead, Brilliant's own methodology, analytical framework, domain expertise and benchmark data provide important guidance for how AI is used in the product.

We utilize sub processors who are adhered to the EU-US Data Privacy Framework. For AI services, we have chosen to use Microsoft Azure OpenAI, which complies with EU regulatory requirements and ensures that our prompts:

- are NOT available to other customers.
- are NOT available to OpenAI.
- are NOT used to improve OpenAI models.
- are NOT used to improve any Microsoft or 3rd party products or services.
- are NOT used for automatically improving Azure OpenAI models for your use in your resource (The models are stateless, unless you explicitly fine-tune models with your training data).
- Models used are fine-tuned Azure OpenAI models and available exclusively for our use.

The Azure OpenAI Service is fully controlled by Microsoft; Microsoft hosts the OpenAI models in Microsoft’s Azure environment and the Service does NOT interact with any services operated by OpenAI, e.g. ChatGPT, or the OpenAI API.

8.1 AI-SUPPORTED MEASUREMENT, INSIGHT AND ACTIONS IN BEAT

Beat supports managers and teams through a continuous cycle of measurement, insight and action. AI is used to support the selection of relevant questions, analyse aggregated survey results, formulate insights and suggest suitable activities. These processes are guided by Brilliant's established methodology and analytical framework.

Question selection is primarily based on previous survey results, trends and Brilliant's methodology. Limited team-level context may also be used to improve relevance, but survey results remain the primary basis for the selection. AI can only select questions from the predefined set configured for the survey. It cannot introduce new survey questions and returned question selections are validated by the application.

Insights are generated from aggregated survey results together with Brilliant's methodology, experience and benchmark data. The purpose of the generative AI model is to help identify, formulate and communicate relevant insights rather than independently determine how survey results should be interpreted.

AI may also suggest activities for the team. Suggested activities are presented as proposals and require an active decision by the manager before becoming active.

Insights from one measurement round may be used as additional context in later rounds, creating a continuous loop between measurement, insight and action.

AI-generated insights are clearly identified as AI-generated content.

8.2 Anonymity and data minimisation in Engage and Beat

The existing anonymity requirements for employee surveys are applied before survey results are made available to AI functionality.

Only aggregated results that fulfil Brilliant's anonymity requirements are used for question selection and insight generation. Personal identifiers, information about individual respondents and free-text survey comments are not included.

AI-generated insights may be translated into the languages used by the customer. Translation is limited to content generated by the application; customer-entered text is not sent to the AI translation functionality.

8.3 Team context – Story in beat

Story is a conversational AI-supported functionality used to collect relevant factual context about a team.

Story is intentionally designed for team-level context rather than information about individual employees. The agent is instructed not to request or store personal data about identifiable individuals or sensitive personal information.

Before Story information is stored, the user is presented with a structured summary and must review and approve it. Stored Story information can subsequently be reviewed and modified by the user.

Story conversations are stored separately from the persistent team context and are retained for a maximum of 24 hours. The persistent Story contains only the structured team context approved by the user.

Story may be used to provide additional context to Beat, for example when formulating insights or distinguishing between otherwise similarly relevant questions. Its role is deliberately secondary to survey results and Brilliant's methodology.

8.4 Data access and AI output

AI functionality follows the same authentication, authorization and tenant-isolation principles as the rest of Insight.

AI-generated content is processed through Brilliant's application layer before it is stored or used by other product functionality. Where applicable, outputs are validated against predefined formats and application rules.

AI is used to support analysis and decision-making at team and organisational level. It is not used to evaluate the behaviour or performance of individual employees or to make decisions regarding recruitment, employment conditions, promotion or termination.

8.5 Risk with the use of AI

Brilliant Future continuously evaluates its use of AI from information security, privacy, quality and regulatory perspectives as part of the company's product governance and risk-management processes.

Relevant risks include incorrect or misleading AI-generated content, inappropriate information being entered by users and excessive reliance on AI-generated recommendations.

These risks are reduced through a combination of data minimisation, existing anonymity controls, Brilliant's methodology and analytical framework, restricted access to customer data, validation of AI outputs where applicable, and human review or activation of AI-generated recommendations.

AI-generated content is clearly identified to users, and AI is used as support for managers and teams rather than as an automated decision-maker about individuals.

Brilliant continuously reviews regulatory developments, including the EU AI Act, and evaluates changes to AI functionality through the same product governance, security and privacy processes used for other product development

9 RISKS COMBINED WITH DATA STORAGE AND PROCESSING

Risk	Probability	Control
Foreign authority raises legal claim in the data and enforce it against the provider or gets lawful access by surveillance	Low	Security measures described in section 6.1 makes information useless and extremely hard to interpret, compare to other open solutions (linked-in, Instagram, facebook etc)
Company confidential information leakage caused by misuse of reports and data extracts from Insight	Medium	Avoid extracts / reports and use built in functionality in Insight instead
External security attack causes unlawful access to data in Insight	High	Web application firewall (WAF) and MS defender for cloud for continuous monitoring and scanning of traffic and resource Continuous development process for quick response and mitigation of risks Monitoring and quick incident management response Strong partnerships in operations, monitoring and security
Data breach caused by internal or external misuse of login information to Insight	High	Monitoring and quick incident management response Possibility to activate enhance security measures (e.g. SSO and MFA)

10 TECHNICAL AND ORGANISATIONAL MEASURES

Brilliant Future has an internal engineering team consisting of Architects, Tech leads, UX designers, and Product Managers. The requirement, discovery, design and development phases consider corporate and customer interests as well as quality-, legal-, security- and privacy compliance, referred to as “product governance”.

The development and delivery phase contain all necessary measures and check points to verify that all requirements are met (functional, non-functional). Regression- , feature- and security-tests are handled in the team manually but also automatically through the build pipeline. A close and daily collaboration with the support-team, the incident manager and operations team exist to monitor incidents, security alerts or breaches.

As a complement to our internal team Brilliant is using external partners for support, maintenance, monitoring, security, and auditing as well as consulting for specific expertise.

Brilliant Future are ISO 27001 certified, meaning there are processes and controls in place, security awareness and controls are constantly in focus, our Information Security Management System (ISMS) describe controls around:

- Governance and organisational security measures
- Product governance and product development
- Technical Security Measures
- Risk Management
- Incident Management and monitoring
- Sub-Processor and Supplier management
- Internal awareness training procedures

10.1 SOFTWARE DEVELOPMENT LIFECYCLE PROCESS (SDLC)

The purpose of the SDLC process is to ensure that all software developed and maintained by Brilliant Future AB is designed, built, tested and deployed securely, in compliance with legal, regulatory and contractual requirements and in alignment with industry best practise. That includes requirements (functional, non-functional, regulatory and legal) design, development, testing, deployment/release, and security

10.2 ROLES AND RESPONSIBILITIES

The software development lifecycle is driven by a cross-functional product and engineering team consisting of Product Managers, Tech leads, Developers, Architects, UX Designers. The daily work is divided into separate cross functional teams (squads) with all roles included to full fill the end-to-end product delivery. Close and daily collaboration with the customer operations team and the incident manager exist for 2nd line support and to monitor any incidents, security alerts or breaches.

Chief Technology Officer (CTO)

- Owns overall technology strategy, security, and compliance in product development
- Approves architectural decisions and key technical investments
- Ensures SDLC aligns with corporate strategy, risk management, and regulatory requirements

Chief Product Officer (CPO)

- Defines product vision, strategy, and portfolio priorities

- Ensures alignment between product roadmap, customer needs, and company objectives
- Oversees product governance process together with CTO and Product Managers

Product Manager (PM)

- Owns the continuous discovery and design process
- Translates business goals and customer needs into clear product requirements
- Prioritizes backlog items and coordinates cross-functional input (UX, Tech Lead, stakeholders)
- Ensures privacy and security considerations are integrated into product requirements

UX Designer

- Designs user experiences that are intuitive, accessible, and consistent with brand standards
- Conducts user research, prototyping, and usability testing
- Collaborates with developers to ensure designs are feasible and user-friendly

Architect

- Designs and maintains technical architecture for scalability, performance, and security
- Participates in product governance and architecture forums
- Ensures adherence to coding standards, patterns, and secure design principles

Tech Lead

- Oversees technical delivery within the team, ensuring code quality and standards.
- Guides backlog refinement from a technical perspective.
- Mentors developers and coordinates with Architects and DevOps.
- Leads code reviews and resolves technical issues.

11 COMMON QUESTIONS REGARDING OPERATIONS, STORING AND PROCESSING OF PERSONAL DATA

Question	Answer	Comment
1. Brilliant shall ensure protection and privacy of Personal Data related to its services in accordance with relevant data proception legislation and regulations	Yes	Brilliant Future is certified according to ISO/IEC 27001:2022. Our policies are documented and implemented across the organisation and according to our Information Security Management System (ISMS)
2. Brilliant shall ensure data transferred through sub-processors outside EU	Yes	Brilliant use Microsoft datacenters within EU (West Europe, Sweden Central). To ensure integrity of personal data Brilliant applies additional security methods, e.g. stored personal data elements encrypted using AES encryption and separated encryption keys (data at rest) Respondent data pseudonymization when storing data Sub-processors outside EU are certified according to the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/s/, n.d.)
3. What is the reason for using cloud services?	Brilliant Future has chosen to use Microsoft Azure to achieve high flexibility, scalability, and at the same time a high security level. Using cloud services is also part of our strategy for sustainability, where we achieve a more efficient and sustainable energy-consumption in the cloud as well as in a data center in Sweden that is powered by renewable energy (Microsoft's data center in Gävle, Sandviken, Staffanstorp)	
4. Personal Data shall be retained for only as long as necessary and handled with full integrity	Yes	Personal data is pseudonymized and encrypted. Anonymized data is used for benchmark purposes. Disposal of customer data is handled either contractual or at requests
5. Password policy and authentication methods	Password requirements is set to a minimum of 8 characters, a combination of lowercase, uppcase, alpha- and numeric characters. SSO supported via Azure AD. MFA supported via SSO	
6. Separated environments between development, test and production	Yes. The environment is managed by the internal team. We use external partners/experts to support in optimization, security and audits	
7. What is the purpose, location and legal mechanisms used through third party sub-processors	**Twilio/Sendgrid** SMS and email invitations and reminders to respondents Covered by and certified under the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/s/, u.d.). **Microsoft / Azure**	

	Services, applications, and operations in Azure/Cloud (e.g., App/Web services, Database/Storage, Functions, Azure OpenAI) Covered by and certified according to the EU-US Data Privacy Framework. (https://www.dataprivacyframework.gov/s/, n.d.) Only datacenters in Sweden and Western Europe /EU **Pendo (EU)** Used for building our help center and to provide customer support and analytics (no respondent data is transferred) Data processing through established DPA specifying terms for data handling and obligations under GDPR **Hubspot (EU)** Customer relationship management and customer support Covered by and certified under the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/s/, u.d.)	
8. Can Brilliant Future ensure secure processing with underlying partners (sub-processing)	Yes	We have ensured underlying sub-processes use same or equivalent security mechanisms to Brilliant Future. Sub-processors outside EU are certified according to the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/s/, n.d.) Only necessary information is passed to underlying partners as part of our design / privacy by design process
9. Can answers in surveys be derived to physical person?	No	We use mechanisms for pseudonymisation, meaning that answers are separated from respondents. Respondents name and email addresses are stored encrypted (data at rest) IP addresses from respondents are not stored. IP addresses from manager- and HR-roles in Insight are logged as part of user sessions.
10. Do Brilliant Future track respondents- and user sessions (e.g. TCP/IP addresses)	Yes/No	Brilliant Future only track specific roles (Managers and HR) in the platform. No respondent sessions are being tracked, logged or saved.
11. Are Brilliant working with an established Incident Management process covering security- and personal data related incidents?	Yes	Business critical incident get escalated to the Incident Team. All according to ISO/IEC 27001 and our ISMS processes
12. High availability and SLA	Yes	Brilliant rely on Microsoft Azure general SLA of 99.9%. The automatic and continuous deployment process described in our SDLC process also secure high availability and security standards as well as rapid feature deployment. This gives an total SLA of **99.5%**

13. Scheduled maintenance or service-windows	No	Cloud and SaaS services allow high flexibility, availability and avoid need for planned maintenance/service windows
14. Does Brilliant have a Business Continuity Plan (BCP) and Disaster Recovery Plan in place	Yes	Brilliants internal infrastructure (office-network, internal workplace etc) is separated from our commercial platforms (e.g. Insight). Insight is a SaaS, IaaS solution that can easily be re-deployed in multiple locations, even local if necessary. Deployment-pipelines are fully automated. The environment has redundancy over multiple geographic locations. Backup policies are established, restore tests are conducted as part of internal review(s) and according to ISMS procedures.

11.1 REFERENCES

Further information about our policies and the Processing of Personal Data can be distributed on the demand and found in:

- Brilliant Future internal Privacy Policy
- Brilliant - General Information Security Policy
- Brilliant - Incident Management Process
- Brilliant – Risk Management Process
- Brilliant – Business Continuity Plan
- Brilliant – Software Development Lifecycle Process