**Brilliant Future**

Classification: Restricted

# INSIGHT – CX, EX

Architecture, Compliance and Security White Paper

## 1 Document Version Control

| Rev | Modified | Modified By | Implemented By | Document Changes |
|---|---|---|---|---|
| 1.0 | 2023-01-10 | Johan Pellbäck | Product management team | New template |
| 1.1 | 2023-02-16 | Johan Pellbäck, Sofie Roos, Torbjörn Alander | Product management team | Product features, Data processing, Risks |
| 1.2 | 2023-02-20 | Fredrik Kronander, Erik Nordenhök, Johan Pellbäck | Product management team | Architecture, Q&A |
| 1.3 | 2023-03-01 | Johan Pellbäck | Product management team | Complimentary information to Q&A, language support, SDLC |
| 1.4 | 2023-03-08 | Johan Pellbäck | Product management team | Complimentary info regarding data storage in Q&A |
| 1.5 | 2023-04-12 | Johan Pellbäck | Product management team, Engineering team | Complimentary info regarding pseudonymisation, encryption, sessions and sustainability in the cloud |
| 1.6 | 2023-04-28 | Johan Pellbäck | Product management team, Engineering team, Dev ops | Added section 5.2.1 regarding backup and data retention |
| 1.7 | 2023-05-02 | Johan Pellbäck | Product management team, Engineering team, Dev ops | Clarification in chapter 8 regarding processing and sub-processors |
| 2.0 | 2023-10-09 | Johan Pellbäck,<br>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,<br>Jonathan Dahlberg | Architecture team | Chapter 5 as part of WAF implementation using Azure Frontdoor<br>Chapter 7 updates in roles and accountability |
| 2.7 | 2025-01-08 | Johan Pellbäck | Product Management Team | Chapter 5.3 regarding logging |

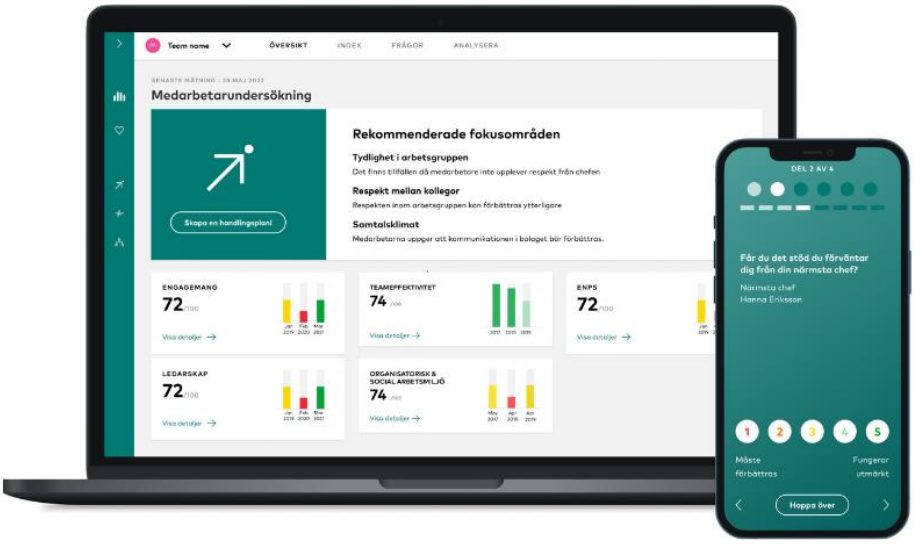
# 2 Document content page

# 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).



Medarbetarundersökning

Rekommenderade fokusområden

Tydlighet i arbetsgruppen

Det finns tillfällen då medarbetare inte upplever respekt från chefen

Respekt mellan kollegor

Respekten inom arbetsgruppen kan förbättras ytterligare

Samtalsklimat

Medarbetarna uppger att kommunikationen i bolaget bör förbättras.

Får du det stöd du förväntar dig från din närmsta chef?

Närmsta chef
Hanna Eriksson

## 3.2 Scope

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

# 4 Products and features

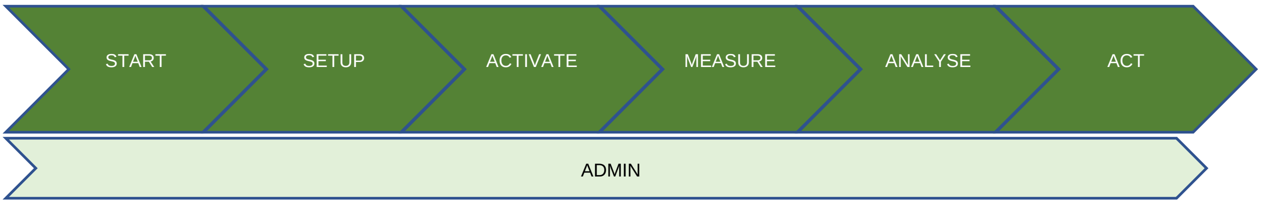
Insight is a web-based solution that supports desktop and mobile devices. With over 20 years of experience in the industry we developed a method that uses engagement as a tool for improvement. Our method is based on scientific studies and our own data. It is proven that our method helps organisations to reach their full potential and become more profitable over time. This is translated into a digital platform that lets employees and managers provide feedback on what works well and what's not. This is presented for HR and managements as insights, with ready to use tools for improvements where it is needed, so they can act on their individual situation.

Today we are supporting a global market in more than 30 languages, targeting medium to large organisations.

The design system is based on the company's graphic profile which can be found in the material we show to our customers. We meet all the requirements for an WCAG AA classification which is essential for creating high availability and a great user experience.

The application is a SaaS solution with the ability to give our customers the full experience and self-service tools to manage organisations, surveys, analytics and reporting as well as other products for managing employee and customer relations.

In section 4.1 we describe a high-level list of features in Insight and the scope of functionalities.



## 4.1 Features

| Feature | Area | Comment |
|---|---|---|
| Login & Start Page | Start | Login using Brilliants Auth over standard TLS/HTTPs or Microsoft Azure AD SSO. Insight is a multi-tenant application that supports logins from Azure AD out of the box using OpenID as the underlying protocol. AD setup is managed by the Brilliant Tech delivery team together with the customer.<br>Start page with white papers, event etc. from https://brilliantfuture.se/insight-hub/. |
| Manage Organisation | Setup | Build the organisational structure through: Excel file uploaded to our SFTP-server (https://sftp.brilliantfuture.se/) then imported by us; batchimport by Excel file directly in the platform; manually in the platform. You can read more about organisation management in our helpcenter. |
| Create & Activate Survey | Activate | Surveys are created and activated by self-service through a survey wizard in the platform. Survey questions are chosen from Brilliants standard library. Customer unique questions can be ordered, once programmed be Brilliant they will be available through self-service in the platform. You can read more about self-service and survey activation in these articles in our helpcenter. |
| Active Survey | Measure | Once activated, you'll be able to view response rate, communication status and mail/SMS bounces. Reminders, end date and reporting date can be edit once activated and participants can be added and removed. You can read more about self-service during an active survey in our helpcenter. |
| Result Calculation & Reporting | Measure | Results are automatically calculated after the chosen survey end date. Users with preview access, normally HR, can preview the result the day after the surveys end date. The result will be reported to managers by mail or SMS on the chosen survey reporting date. Only users with HR or manager permissions will have access to the result. |
| Survey Data Collection | Measure | Survey data is collected by a respondent unique link sent by e-mail or SMS. In lack of e-mail and phone number, a team unique PIN can be generated and entered at https://www.brilliantinsights.se/pin-code-logon. Brilliant will |

| | | |
|---|---|---|
| | | automatically send the PIN and the PIN-link by e-mail or SMS to the manager of the team in question. Any further distribution is then to be solved by the customer. |
| Results | Analyse | Results are presented to HR, Managers and other Stakeholders in your organization.<br>**For employee and leadership surveys (EX):**<br>Managers are only allowed to view results for their own team or teams and compare them to aggregated result above them in the organisational hierarchy. Recommended focus areas can be presented, depending on which questions have been chosen in to include in the survey. Index results can be exported to PowerPoint, question results to PDF and heat map to Excel. Action-plans and deeper analysis is also available to further work with the results and improve your organization.<br>**For customer surveys (CX):**<br>Stakeholders are allowed to see results by analysing customer response, comments, NPS results etc. AI is used for deeper analysis of customer response and to give you deeper understanding of the results. NOTE that results in a customer survey is not anonymous as it is for employee and leadership surveys.<br>You can read more about how to understand the results in our helpcenter. |
| Action plans, Brilliant Workshop and Close the loop | Act | **For employee and leadership surveys (EX):**<br>Action plans can be created in connection to a specific survey or stand alone. Statistics can be viewed and filtered in order to get an overview of which teams are working with the results. It is also possible to use AI to analyse results and to get recommended actions.<br>**For customer surveys (CX):**<br>Stakeholders can analyse results, answers and close the loop with customers. AI is also used for deeper analysis of aggregated results and comments. |

| | | |
|---|---|---|
| | | You can read more about action plans and Brilliant workshop in our helpcenter. |

### 4.1.1 Anonymity for Employee surveys (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://help.brilliantinsights.se/hc/en-150/articles/360013325558-Anonymity-rules.

### 4.1.2 Languages

Insight supports multiple languages for administrators and for the survey. We have a separate process for adding languages to the survey part, and this could for specific request require an extra cost to our customers.

The admin part (managers, HR 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 here: Brilliant Produktbeskrivning EX | Brilliant (brilliantfuture.se)

(* = require extra cost)

## 4.2 Web Connectivity Accessibility Guidelines (WCAG)

Brilliant Future is dedicated to meet the accessibility guidelines according to WCAG AA 2.1. Below is a explanation of we fulfil these requirements, as well as identified deviations:

### 4.2.1 In general

Graphical Elements and Design: All graphical elements on our platform meet the necessary colour contrast and font size requirements to be considered accessible according to WCAG AA 2.1.

Deviation: Some graphs may lack alternative text, which can affect users who rely on screen readers.

### 4.2.2 Results Pages

Our results pages are designed to support the requirements needed to be WCAG AA 2.1 compliant.

Deviation: Some elements may lack alternative text, impacting accessibility for users with visual impairments.

### 4.2.3 Text Readability

All text presented on our platform strives to maintain a LIX value (Readability Index) between 40-60 to ensure good readability.

Deviation: Some system texts and error messages may have a higher LIX value, making them more difficult to understand.

### 4.2.4 Survey

Our surveys are specifically designed to achieve a high level of accessibility and are crafted for a broad user group. This means they support all requirements for WCAG AA 2.1 and 2.2, with some deviations.

Deviation: Minor deviations may occur, but we continuously strive to minimise these and improve accessibility.

### 4.2.5 Supported Devices

We support the use of our platform on Desktop, Tablet, and Mobile. The mobile version is optimised for surveys and results pages, while deeper analyses, system setups, and management are recommended to be performed on a larger screen.

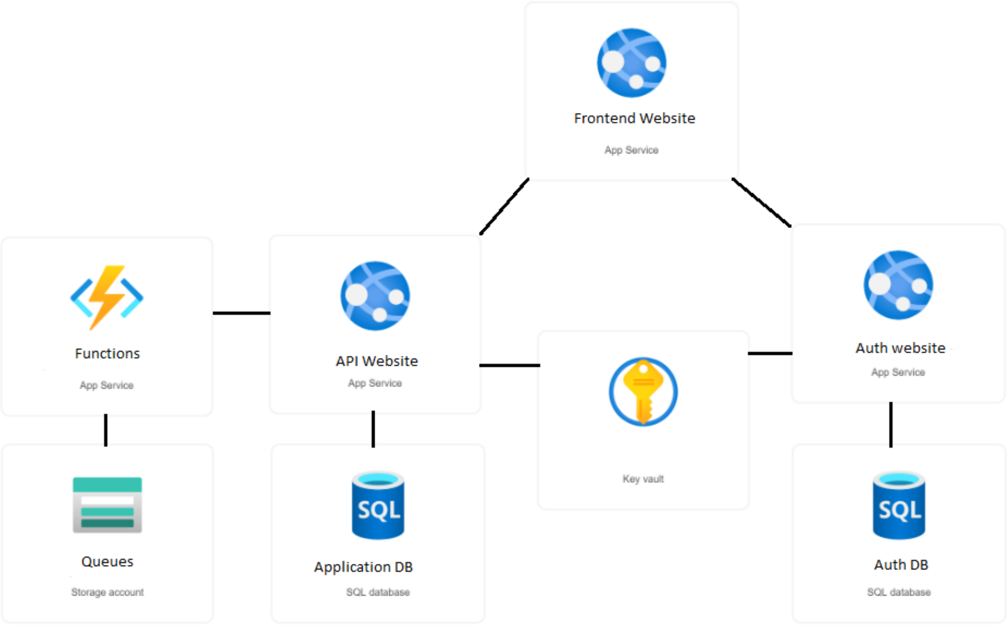
### 4.2.6 Summary

Brilliant Future is committed to meet and exceed the accessibility requirements according to WCAG AA 2.1. We conduct regular reviews and updates to ensure our platform remains accessible to all users. We are aware of the current deviations and are actively working to address them and enhance the user experience for everyone.

# 5 Architecture

Insight is a 100% SaaS application hosted in the cloud using Microsofts Azure. This gives our customers full reliability, scalability and flexibility. We use industry standard components to create a secure and stable environment and together with our MS certified partners we continuously monitor and evaluate the environment for best performance and optimization.

## 5.1 Deployment view



Frontend application is an angular site hosted on an app service and is the main touchpoint for customers. For credential management, login and SSO integrations we use auth website hosted in a separate app service with a separated database.

The main API which the frontend communicates with is hosted in a third app service which connects to the main database of the application as well as an azure function with a storage account for asynchronous tasks.

All security keys and encryption secrets are handled by a key vault.

## 5.2 Security

### 5.2.1 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.

### 5.2.2 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.

## 5.3 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.

### 5.3.1 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)

### 5.3.2 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

### 5.3.3 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.

## 5.4 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

### 5.4.1 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.

## 5.5 Integrations

The most important thing for a successful implementation of Insight, regardless of whether it concerns customer- or employee surveys, is to build your organisational structure and to find the right structure for reporting and analysis.

### 5.5.1 File import

We primarily use file imports to integrate our customer organisational data. The main reason for using file imports is that most of our customers need a different way of reflecting the organisation and how to build hierarchy and relations between entities.

Another reason for using file imports is when organisations have small teams that may cause limitations when anonymity rules are applied.

Examples of how to use file imports:

- Continuous imports – using a standardized template with users and teams, mapping of customized attributes (team, manager-id, parent/child attributes etc).
- Manually - manually build organisational hierarchy, file-import of user-data.
- Batch-imports – a even more seamless way of continuously importing user-data on an existing organisational structure.

### 5.5.2 API integrations

Integrations to Azure Active Directory (AD) and Alexis HR exist.

### 5.5.3 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. Our recommendation is to start building the structure using a file export/import.

Always consider the following:

- 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://help.brilliantinsights.se/hc/en-150/articles/360013325558-Anonymity-rules
- 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 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.

## 6.1 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 North Europe (Ireland), 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).

## 6.2 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 | Anonymised |

| | | |
|---|---|---|
| | credentials separately with references to encrypted usersIDs | |

## 6.3 Secrecy, Privacy and AI

For Brilliant Future, privacy and integrity are major focuses. Our use of AI contributes to both an improved user experience and deeper insights about our customers and our customers' clients and employees, while also protecting personal data and individual privacy.

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[1].

## 6.4 Risks combined with data storage and processing

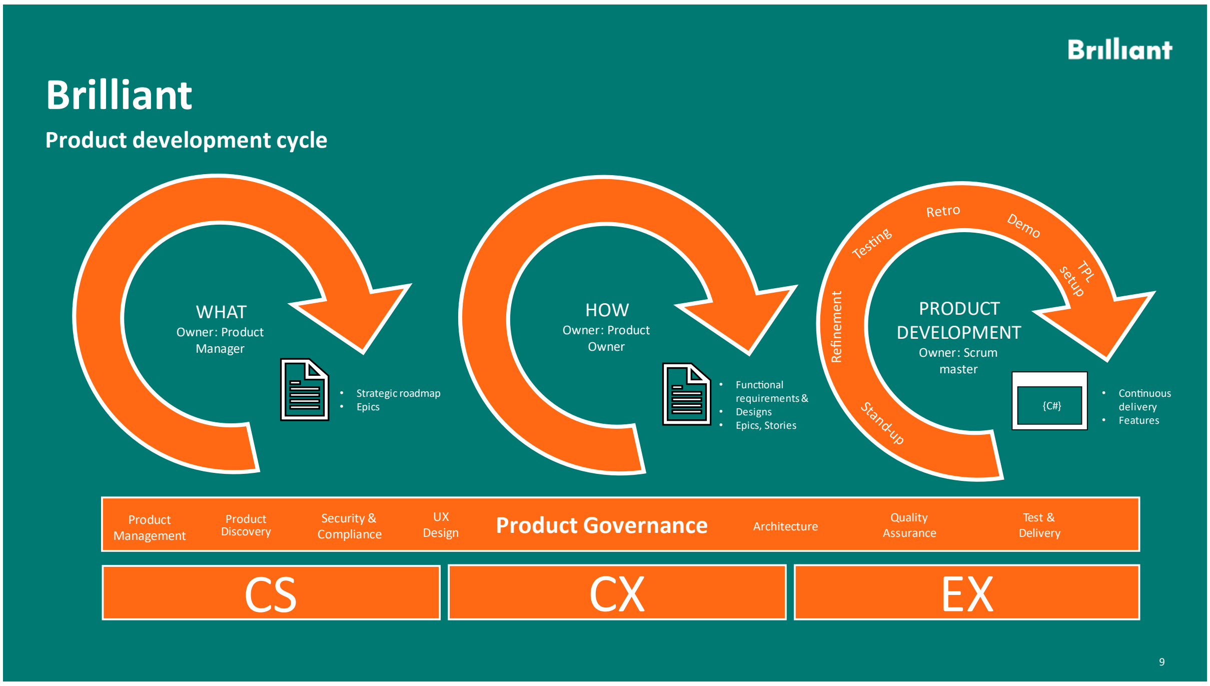
| Risk | Probability | Control |
|---|---|---|
| Foreign authority raises legal claim in the data and enforce it against the provider or gets lawful access by surveillance | Low | Security measures described in section 6.1 makes information useless and extremely hard to interpret, compare to other open solutions (linked-in, Instagram, facebook etc) |

[1] https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy

| | | |
|---|---|---|
| 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<br>Continuous development process for quick response and mitigation of risks<br>Monitoring and quick incident management response<br>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<br>Possibility to activate enhance security measures (e.g. SSO and MFA) |

# 7 Technical and organisational measures

Brilliant Future has an internal engineering team consisting of Architects, Tech leads, UX designers, QA-engineers, and Product Owners. The requirement, discovery, design and development phases (what, how, development) consider corporate and customer interests as well as quality-, legal-, security- and privacy compliance, referred to as "product governance".



Brilliant

Brilliant

Product development cycle

WHAT
Owner: Product Manager

- Strategic roadmap
- Epics

HOW
Owner: Product Owner

- Functional requirements & Designs
- Epics, Stories

PRODUCT DEVELOPMENT
Owner: Scrum master

Retro
Demo
TPL setup
Testing
Refinement
Stand-up

{C#}

- Continuous delivery
- Features

Product Management
Product Discovery
Security & Compliance
UX Design
Product Governance
Architecture
Quality Assurance
Test & Delivery

CS
CX
EX

9

The development and delivery phase contain all necessary measures and check points to verify that all requirements are met (functional, non-functional). Manual and automatic regression and security tests are handled by the QA-team. A close and daily collaboration with the support-team, the incident manager and operations team exist to monitor any 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.

## 7.1 Software development lifecycle process (SDLC)

Brilliant Future uses an established SDLC process documented in our ISMS library. In general the organization's Software Development Life Cycle (SDLC) includes the following phases (see SDLC process document for further details):

- Discovery and design
  - Requirements Analysis
  - Architecture and Design
  - Refinement

- Construction and development
    - Development
    - Testing
- Change management
    - Change request and approval
    - Change register
    - Change risk assessment
    - Deployment/Release
    - Decommission
- Operations/Maintenance/Monitoring

## 7.2 Roles and accountability

Brilliants tech-, delivery and product management team consists of senior roles (e.g. Product Managers, Product Owners, Product Designers, Architects, Front-end/Back-end engineers). Specific roles are assigned to measure quality, performance, security and to manage and maintain daily operations (eg QA-leads, Test managers, Scrum master, Dev ops, Technical Project managers).

**The management team** at Brilliant Future (through the CEO) is ultimately responsible and accountable for ensuring that objectives of the policy are met.

The **CTO** is responsible for implementation of policies according to ISO using the Information Security Management System (ISMS).

The **DPO**-role is held by our CTO, our legal partner is responsible for regulating activities to achieve objectives related to compliance and GDPR.

**Architects** and **Tech leads** is responsible for implementation technical designs according to functional- and non-functional requirements

**QA** is responsible for assuring quality in all parts of the development process.

Security partners conduct yearly security assessments (penetration and vulnerability tests) and continuously monitor our environment for any security breaches.

# 8 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 working according to ISO 27001 and 27701. The aim is to reach official certification<br>Our policies are documented and implemented 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).<br>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)<br>Respondent data pseudonymization when storing data<br>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 | Yes | Personal data is pseudonymized and encrypted. Anonymized data is used for benchmark purposes. Disposal of customer |

| | | |
|---|---|---|
| handled with full integrity | | 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**<br>SMS and email invitations and reminders to respondents<br>Covered by and certified under the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/s/, u.d.).<br>**Microsoft / Azure**<br>Services, applications, and operations in Azure/Cloud (e.g., App/Web services, Database/Storage, Functions, Azure OpenAI)<br>Covered by and certified according to the EU-US Data Privacy Framework. (https://www.dataprivacyframework.gov/s/, n.d.)<br>Only datacenters in Sweden and Western Europe /EU<br>**Pendo (EU)**<br>Used for building our help center and to provide customer support and analytics (no respondent data is transferred)<br>Data processing through established DPA specifying terms for data handling and obligations under GDPR<br>**Hubspot (EU)**<br>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.<br>Sub-processors outside EU are certified according to the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/s/, n.d.)<br>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.<br>Respondents name and email addresses are stored encrypted (data at rest)<br>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 |
| 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.<br>Deployment-pipelines are fully automated. The environment has redundancy over multiple geographic locations. |

## 8.1 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