BlueBee Data Security & Compliance

Data security and protection are of the utmost importance as genomics and related subject data are sensitive. Data security and compliance are the cornerstones of BlueBee. All technologies and services that BlueBee delivers adhere to the guidelines described in this document, in support of BlueBee customers and those that they impact.

Table of Contents

Overview

Data security and information protection are becoming increasingly important in this digital age. The incorporation of new and complex technologies such as server, cloud, and internet for data sharing and storage makes information security challenging, particularly as it pertains to human data. Indeed, genomics data processed for clinical and research purposes is subject to local data privacy and regulatory compliance requirements, which add additional independent complexities to the management of data safety.

BlueBee's services, including its Genomics Platform, Web Applications, and data center partners are compliant with all applicable local and global regulations and standards. This guarantees customers comprehensive data security and regulatory compliance. The combination of BlueBee's sophisticated Genomics Platform data center infrastructure and certification compliance, allows BlueBee to meet even the most stringent security requirements of customers who work with sensitive information such as patient-derived sequencing data.

Compliance With Data Protection And Security Requirements

This document details how BlueBee ensures its clients' compliance with data protection and security requirements when using BlueBee's cloud-based accelerated genomics analysis platform for fast, efficient, and affordable processing of large volumes of clinically relevant sequencing data.

This document is divided into five sections:

1. An overview of the security measures implemented by BlueBee's private cloud-based accelerated genomics analysis platform.

2. An overview of the mechanisms that guarantee data availability while addressing specific cloud processing requirements.

3. An overview of BlueBee's conformity with data protection & privacy standards.

4. An overview of BlueBee's compliance with data protection & privacy regulations.

5. A summary of the measures taken to ensure that BlueBee's clients can reliably use the cloud-based genomics analysis platform in a manner which is compliant with applicable data protection legislation.

BlueBee's Genomics Platform Security Measures

Extensive security measures have been implemented to ensure the highest level of protection of sensitive human genomics data. BlueBee's Genomics Platform is designed to ensure complete data security and privacy, to meet all regulatory requirements, to control both institutional and enterprise fine-grained access, and to ensure the integrity of data flow across the entire platform whether processed on the cloud, transferred via the internet, or stored at rest. The platform was designed with multi-layered data security in mind, with the purpose of accommodating confidential patient information. This ensures a platform that complies with even the strictest of security controls.

BlueBee's Platform is deployed on a private cloud and runs on dedicated servers, ensuring the highest degree of isolation, which is also typically a pre-requisite for High Performance Computing. In addition to physical security controls, the analytics pipelines are executed within a container to ensure they stay within boundaries that are set out by the platform; this includes access to data and resource consumption. This combination allows BlueBee to deliver high-caliber platform and infrastructure security without compromising performance, which is superior to the use of a Virtual Cloud. Furthermore, this combination offers virtually unlimited scaling capacity for sequencing data analysis and storage.
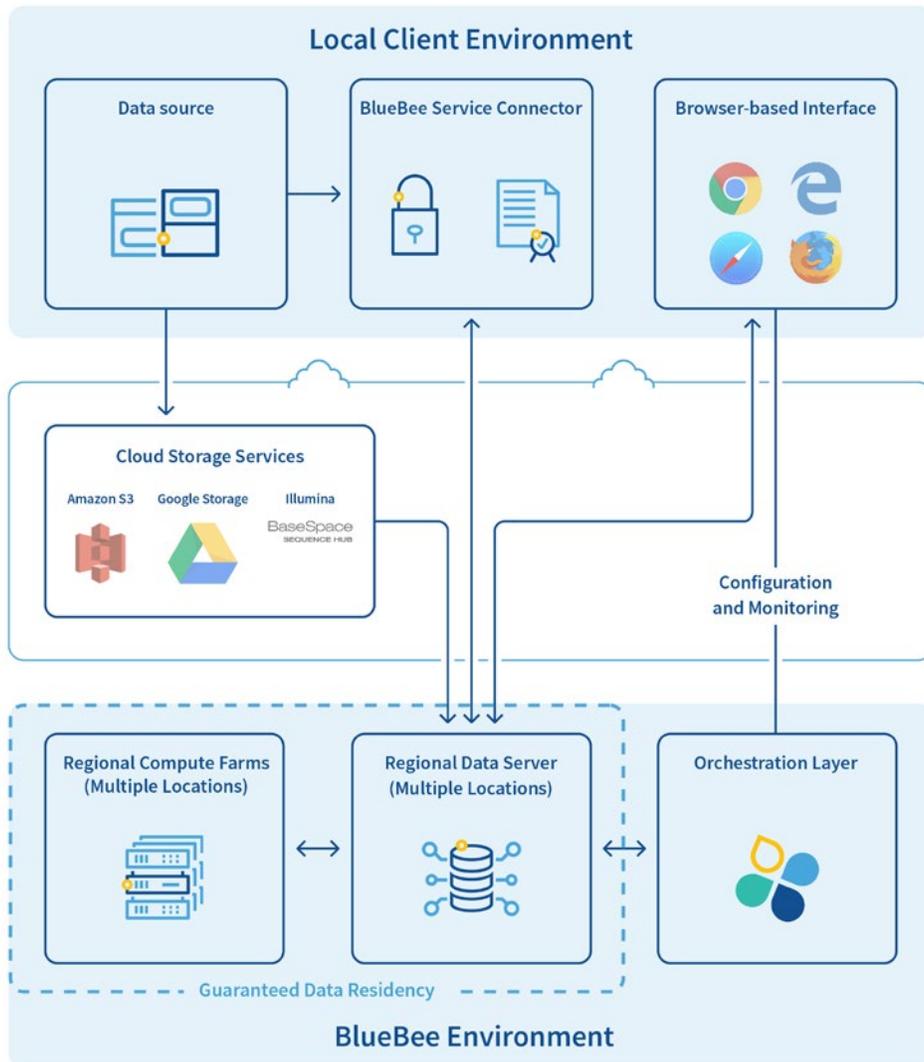

Figure 1: BlueBee Genomics Platform building blocks overview

BlueBee's Data Security Levels

Below are the multiple security features embedded within BlueBee's Genomics Platform.

Security Features	BlueBee Genomics Platform	Advantages
Two-factor authentication	Step authentication for sensitive actions*.	Ensures the highest-level confidentiality
Login policies	Strong password, renewal period, & inactivity timeout enforced.	Ensures the highest-level confidentiality
Data anonymization	Enables storage of anonymized patient data alongside data files. Allows the use of patient data throughout the processing chain or the use of a reference link back to the patient's data held at the client's supporting infrastructure.	Ensures data privacy throughout all actions
Object classification	By default, any object** is owned by the user who first introduced the object to the platform. The owner of the object**, via owner privileges, controls fine-grained access to the object by other users, companies, and communities.	Ensures fine-grained access privileges
Audit trailing	All actions, for all objects within the platform, are recorded (including viewing an object).	Ensures regulatory requirements are met
Four-eyes control	Sensitive actions must be approved by two users with appropriate access permissions. In combination with step-up authentication. Applies to sensitive actions* on shared data and access-granting to permitted data**.	Protects sensitive data and actions
Role-based access	A complex matrix allows the client's administrators to setup granular security definitions to fit organizational requirements. Fine-grained security controls allow tight regulation over who can do what within the platform – applies to all objects**.	Allows an administrator to implement organizational control requirements
PKI infrastructure (Public Key Infrastructure)	Integrates digital certificates, public-key cryptography, and Certification Authorities into an enterprise-wide network security architecture. This framework allows the generation, production, distribution, control, accounting and destruction of public key certificates.	Provides digital signature and encryption capabilities Ensures the integrity of data**flowing across the entire platform Ensures regulatory requirements are met
Data encryption	All data is encrypted in transit (TLS) and at rest (AES 256/128). Furthermore, (1) the integrity of the data is validated before any action is performed, which includes data download and use of data as input for a pipeline; (2) in the event of a data breach, BlueBee's security officers, will be alerted and the data will be quarantined. Once the root cause has been identified, appropriate actions will be taken.	Ensures data privacy when transferred over the internet, processed on the cloud, and stored at rest

* Data is defined as data sets and pipelines; Object is defined as any record in the database.

** Sensitive actions include modifying a pipeline, uploading, and configuring data. sensitive actions include modifying a pipeline, uploading, and configuring data.

Comprehensive Platform Security Architecture

BlueBee's high performance genome analysis platform is a private cloud-based solution with industrial-level security. This platform supports high performance and highly scalable sequencing data processing and storage capacity for individuals or enterprises in the clinical, pharmaceutical, or research domains.

Key capabilities:

1. Direct and secure integration with sequencing instruments and infrastructure for transparent and efficient data upload and processing within a diagnostics workflow.

2. Highly configurable, flexible, and extensible sequence data analysis pipelines, enabling bioinformaticians to run version-controlled sequence data analyses.

3. On-demand scalable sequence data analysis via parallel processing of pipelines which can support potential surges in data analysis when needed.

4. Feedback-loop based job monitoring and job prioritization, which allow for quick adjustments to clinical requirements and research findings.

5. Instantaneous delivery of data interpretation for expedited insight gathering.

The analytics pipeline capabilities support streaming, as well as batch processing of large data sets without compromising processing duration, latency or efficiency. Large volumes of data are processed within the platform in a secure, private and encrypted manner, complying with all relevant regulatory requirements.

To ensure comprehensive data privacy and compliance with all relevant regulatory requirements the following actions apply:

1. BlueBee's Genomics Platform runs on dedicated servers with the highest degree of isolation, as the machines are exclusively used by BlueBee.

2. BlueBee's analysis pipelines are executed within the confines of a container, which ensures that they stay within the boundaries that are set out by the platform; this includes access to data and resource consumption.

3. BlueBee's private cloud operates in multiple geographic regions and provides users with elaborate functionality for audit trails, encryption, data storage and retrieval.

The three elements listed above allow BlueBee to deliver superior platform and infrastructure security without compromising performance. Furthermore, this combination offers virtually unlimited scaling for data analysis and storage.

BlueBee's primary security goal is to allow only authorized users the access to safely contained and isolated data.

Global Data Center Deployment

To comply with local regulations, BlueBee offers a distributed model whereby genomics data files and any related meta-data can be stored in the region of choice. To accomplish this, BlueBee operates globally distributed high-performance computing centers. Access to the data is regulated by the central platform, but the actual genomics data flow, which includes data download and data view, occurs between the browser and the regional webserver directly.

Figure 2: Truly global deployment in regional datacenters

Processing and storage of genomics data are contractually guaranteed to be in the user's region of choice through, "Data Residency Control". This type of control mechanism is essential for compliance with local regulatory requirements, which state that genomics data cannot leave a defined region and needs to be operated according to local data privacy regulations.

This global distribution model allows BlueBee's platform to store data and perform computational analysis within a location close to the data source and thus to meet regulatory compliance for data storage locality. This means, that when a client sets up a new project, the specific location can be selected. The strategic global reach of the platform allows for data to be processed and stored in one of the locations currently supported worldwide.

The Data Residency Control feature allows users to have a single interface for managing projects and data processing across the globe. Data residency is assured without the burden of managing multiple data centers separately while allowing for secure collaboration and data sharing.

Europe	Americas	Asia Pacific
The Netherlands	CA, USA	Australia
Belgium	DC, USA	China
England	IA, USA	Hong Kong
Finland	NC, USA	India
France	NY, USA	Indonesia
Germany	OR, USA	Japan
Italy	SC, USA	Korea
Norway	TX, USA	Singapore
Spain	WA, USA	South Korea
Switzerland	VA, USA	Taiwan
	Brazil	
	Canada	
	Mexico	

Guaranteed Availability And Specific Cloud Processing Requirements

The detailed summary of security safeguards within this section demonstrates BlueBee's dedication to offering a cloud-based accelerated genomics analysis platform to customers who need to process genomics data in a compliant, secure, and reliable manner.

When processing genomic data, the infrastructure must be always available and highly secured. For this reason, BlueBee carefully selects reliable data center partners that guarantee a high-level of data availability. Furthermore, BlueBee actively ensures that its platform can operate within those data centers in accordance with the highest level of security requirements. These specific requirements relate to availability, integrity, confidentiality, transparency, data isolation, portability, and accountability.

Requirements	BlueBee Solution	Advantages
Availability	Partnering with reliable data centers	Guarantees dedicated network connectivity, redundancy, uninterruptable power supply (UPS), and effective data backup strategies
Integrity	PKI infrastructure	Ensures the originality and integrity of the data flow across the entire platform Assures regulatory requirements are met
Confidentiality	Data encryption "in transit" (TLS) and "at rest" (AES256/128)	Ensure data confidentiality
Transparency	Complies with client-specific data residency requirements	Discloses data center locations
Data isolation	Industry standard data segregation techniques	Ensures data is not accidentally shared or disclosed with a 3rd party
Portability	Standardized tools for data output	No vendor lock-in with no legal impediments to exporting client data
Accountability	Mechanisms to ensure IT accountability	Logs all activities at all times

Availability

As with many Information and Communication Technology (ICT) agreements, availability is a key issue when assessing the quality of a cloud computing agreement.

BlueBee understands that in the context of cloud computing services, internal and external availability risks exist. Therefore, BlueBee built in a business continuity and a disaster recovery plan into its business process. BlueBee's Genomics Platform is supported by BlueBee's business continuity and disaster recovery plan. The platform is installed on a high-availability private cloud infrastructure in ISO/IEC 27001:2013 certified facilities, which adhere to the Uptime Institute's Tier III design standards.

Data security and redundancy are protected by BlueBee's proprietary failover application, which is dependent on a central platform established as an active / passive setup distributed across two data centers. In the event of a disaster, the central platform is transferred to the backup node.

The Recovery Time Object (RTO) for such a failover is 6 hours, while the Recovery Point Objective (RPO) is zero and is achieved immediately by synchronously directing the production database towards the backup database.

Integrity

Given the nature of the data, e.g. sensitive human genetics information, integrity is of the highest importance, irrespective of whether the data is used in a cloud environment. To ensure complete data integrity, BlueBee utilizes a PKI infrastructure (Public Key Infrastructure) designed to verify data integrity before any actions within its cloud-based platform are executed. BlueBee's service description provides additional details on how BlueBee helps its clients process their data in a reliable manner, thereby ensuring data integrity.

Confidentiality

Confidentiality of highly sensitive information is often identified as a key risk factor in the context of public cloud computing services. To ensure confidentiality of all data being processed in BlueBee's cloud environment, data is encrypted both "in transit" and "at rest".

Specifically, BlueBee has implemented a mechanism whereby all personal data that is processed within its Genomics Platform is encrypted.

Given the purpose of BlueBee's private cloud-based accelerated genomics analysis platform, ensuring a high level of confidentiality is an extremely important component in defining the choice of a service provider. Therefore, in addition to data encryption, BlueBee has implemented the necessary access controls to limit unauthorized access to its platform. This helps to further ensure confidentiality by means of identity and access management using strong authentication mechanisms. It is also suggested that the processor's employees and contractors are bound by confidentiality obligations.

Importantly, all BlueBee employees and contractors are bound by confidentiality obligations.

Note: | *For specific information, some controllers might consider so-called "zero knowledge" solutions, whereby the cloud service provider does not have access to the encryption keys and therefore, cannot access the decryption of the hosted information. Even though this greatly decreases confidentiality risks, the use of "zero knowledge" solutions is not mandatory. Alternative arrangements may be made to ensure confidentiality, such as additional contractual and organizational safeguards.*

Transparency

BlueBee can disclose the location of the data centers being used to provide services to any client. Particularly, BlueBee's cloud-based solution was designed to comply with its clients' specific data residency requirements and therefore the solution allows for the geographical identification of the data centers providing client services.

Isolation (Purpose Limitation)

The specifics of a public cloud infrastructure pose additional risks to the data being processed on this infrastructure. Notably, because the same physical hardware is often used for several clients (e.g. memory and storage), data protection authorities perceive this situation as a risk in terms of erroneous disclosure of personal data to other clients. To address this risk, data protection authorities require stringent measures in relation to "data isolation". These measures include implementation of the need-to-know principle, enforced through technical and organizational measures (incl. access limitation and role-based access). This includes measures that ensure data segregation, i.e. by containerizing the stored data.

To ensure data is not accidentally disclosed to other parties as a result of processing activities on BlueBee's Genomics Platform, BlueBee follows industry standard data segregation techniques. Furthermore, BlueBee's cloud-based platform restricts access to data by using role-based access restrictions and logging. To protect particularly sensitive data and actions, techniques such as anonymization, four eyes control and full audit logging functions are included in the platform. For more details, see the section "BlueBee's Data Security Levels" above.

BlueBee Data Encryption

In transit	TLS
At rest	AES256/128

Portability and Exit-Management

Data protection authorities particularly focus on data portability and exit-management. BlueBee's cloud-based platform was specifically designed to ensure data processed by means of the platform is always available to its clients. The platform makes use of standardized tools for its output. Consequently, there is no risk of vendor lock-in. Vendor lock-in is where the client can neither migrate to another cloud service provider nor insource the service because of lack of interoperability.

BlueBee does not use proprietary data formats and interfaces, as other cloud providers might do, because these formats can result in a situation of vendor lock-in. BlueBee's terms and conditions clearly stipulate that the client remains the owner of the processed data. Therefore, there are no legal impediments that would prevent a client from exporting his/her data at any time. BlueBee commits to destroying client data at the end of an agreement in accordance with applicable industry standards. This obligation also serves to ensure the privacy of client's data and to reinforce the purpose limitation principle.

Accountability

To ensure cloud-based data processing is logged at all times for all activities, BlueBee's cloud-based platform provides the required mechanisms to ensure (IT) accountability.

International Data Transfers And Data Residency Requirements

Since BlueBee is based in the European Economic Area (EEA) with data centers also located in the EEA, the restrictions on international data transfers do not apply when personal data is being processed by BlueBee's genomics platform. Therefore, BlueBee's EU presence is a substantial regulatory and practical advantage. With that in mind, international data transfers can validly be organized under the GDPR, even though criticism remains with regards to some of the legal instruments that allow international data transfers.

Note: *Data protection requirements do not impede the use of cloud services within the European Economic Area due to the fact that the GDPR (EU) 2016/679 has created an internal market that allows, in principle, the free flow of personal data. It should be noted that the transfer of personal data to third countries (i.e. countries outside the European Economic Area) not offering an adequate level of protection is prohibited, unless additional safeguards are implemented. Such additional safeguards may be the use of contractual clauses authorised by the competent supervisory authority; or standard data protection clauses in the form of template transfer clauses adopted by the Commission.*

National member state law may impose stricter data residency requirements for specific entities (e.g. hospitals) or special categories of data (e.g. genetic data). These restrictions do not result from applicable data protection laws.

Generally, BlueBee's platform can be deployed in data centers located in the same region as the controller's establishment, as detailed in the section on Global Data Center Deployment. Therefore, BlueBee's cloud-based genomics platform complies with these additional legal and regulatory restrictions which are imposed on processing and storage of such data in the member state of the controller.

BlueBee Certifications

BlueBee is committed to demonstrating its conformity with applicable data protection, security and quality requirements. BlueBee has, therefore, obtained various internationally recognized standards, including ISO/IEC 27001:2013.

The following table demonstrates BlueBee's certifications with applicable data protection, security and quality standards.

Certification	Description
ISO/IEC 27001:2013	International standard for managing risks to the security of information. Certification to ISO/IEC 27001 proves that you are managing the security of your information. The standard adopts a process-based approach for establishing, implementing, operating, monitoring, maintaining, and continually improving an information security management systems.
NEN 7510-1:2017	Dutch standard for information security management in healthcare in the Netherlands. Part 1 of the standard contains requirements for establishing, implementing, maintaining and continuously improving an information security management system relating health informatics.
CSA STAR Level One	Detailed compilation of global industry-based standards for cloud services provided by the Cloud Security Alliance (CSA). CSA Security Trust, Assurance and Risk (STARTM) is the industry's most powerful program for security assurance in the cloud. It encompasses key principles of transparency, rigorous auditing, and harmonization of standards.
HDS:2018	Standard introduced by the French governmental agency for health, 'Agence Française de la Santé Numérique' (ASIP Santé). The Health Data Hosting (HDH) or commonly known as 'Hébergeur de Données de Santé' (HDS) certification, aims to strengthen the security and protection of personal health data.
ISO 13485:2016	International standard for medical devices that specifies requirements for a Quality Management System, where an organization needs to demonstrate its ability to provide (*in vitro* diagnostic) medical devices and related services that consistently meet customer and applicable regulatory requirements.

BlueBee is confident that these certifications can be presented in lieu of a case by case assessment by controllers. By offering this comprehensive spectrum of data security certifications, BlueBee reduces the administrative and financial burden for its clients.

BlueBee is ISO/IEC 27001:2013 Certified

BlueBee is ISO/IEC 27001:2013 certified by an independent auditor for the full scope of its activities which includes development, management, and support of a cloud-based analysis platform for processing of large volumes of omics and health data. In compliance with the ISO/IEC 27001 standard, BlueBee constructed an Information Security Management System (ISMS) to secure business operations managed by its platform and other supporting processes.

Controls covering all areas of information security implemented:

- Security awareness and training
- Monitoring
- Access control and accountability
- Disaster recovery planning
- Authentication
- Incident response

- Equipment maintenance
- Secure media handling
- Physical and environmental security measures
- Risk management
- Systems and network security

BlueBee maintains policies and procedures detailing how the abovementioned controls are executed.

- **ISO/IEC 27001** is an international security standard that outlines the requirements for information security management systems and provides a systematic approach to managing company and customer information based on periodic risk assessments.
- **ISO/IEC 27002** consists of best practices which support and contribute to ISO 27001 compliance.

BlueBee is NEN 7510-1:2017 Certified

NEN 7510-1:2017 is the Dutch standard for information security for organisations handling patient data. The standard consists of a combination of ISO/IEC 27001, ISO/IEC 27002 and ISO 27799 controls, with additional controls specific to health information such as two-factor authentication and information labelling. The implementation of the specific controls provided by NEN 7510-1:2017 emphasise BlueBee's commitment to security, in particular with regards to patient data and local regulatory compliance requirements.

NEN 7510-1:2017 includes the following:

- Risk management
- Approach to the Information Security Management System
- Information Security Policy
- Organisation of information security
- Asset management
- HR Security
- Physical and Environmental security

- Communications & Operations Security
- Access Control
- Information Systems, Acquisition, Development and Maintenance
- Information Security in Incident Management
- Business Continuity Management
- Compliance

The scope of BlueBee's NEN 7510-1:2017 certification mirrors the scope of its ISO/IEC 27001:2013 certification: 'Develop, manage, and support a cloud-based analysis platform for processing of large volumes of omics and health data'. This certification is valid for 3 years with annual surveillance assessments.

BlueBee is HDS:2018 Certified

The French Public Health Code (Article L.1111-8) requires that IT managed service providers that host Personal Health Information (PHI) obtain 'Hébergeur de Données de Santé' (HDS) certification. The certification reference system was introduced by the French governmental agency for health, l'ANS (l'Agence du Numérique en Santé) and provides a framework to strengthen the security and protection of PHI. This reference system is also referred to by the term Health Data Hosting (HDH) reference system.

BlueBee obtained HDS:2018 certification by successfully completing the conformity assessment procedure executed by the independent certification body, BSI France. BlueBee's ISMS governs health data hosting activities, including development, management, support and maintenance of cloud infrastructure and cloud-based information systems that process large volumes of omics data and health data.

Bee's ISMS conforms to HDS:2018 and incorporates requirements from:

- ISO 20000 (Service management system)
- ISO/IEC 27001 (Information security management systems'
- ISO/IEC 27017 (Information security controls for cloud services)
- ISO/IEC 27018 (Protection of personally identifiable information)
- Specific requirements for health data hosting

BlueBee is officially listed on the ANS's website as an HDS-certified host, covering the following health data hosting activities:

- The provision and maintenance in operational condition of the application platform hosting the information system.
- The provision and maintenance in operational condition of the virtual infrastructure of the information system used for the processing of health data.
- The administration and operation of the information system containing the health data.
- Backup of health data.

BlueBee works closely with HDS certified providers of physical cloud infrastructure in order to ensure the entire supply chain is HDS certified. This ensures that companies working within the French healthcare industry can confidently exchange, store and process data pertaining to French PHI using BlueBee as a health data hosting provider. Make sure you request the extensive list of geographical regions in which BlueBee can provide their HDS certified services.

BlueBee is CSA STAR Level One Certified

BlueBee has achieved Level One certification for the CSA STAR Assessment, which demonstrates BlueBee's ongoing commitment to platform and data security. In compliance with Level One of the CSA STAR Assessment BlueBee customers can rest assured that the highest level of cloud security is in place, thus addressing various security concerns.

Security aspects implemented cover:

- User interface
- Data and data center security
- Data and access management
- Governance and risk management
- Interoperability with other tools
- Low threat and vulnerability risk
- Mobile security
- Interface security

BlueBee maintains policies and procedures detailing how the above-mentioned controls are executed.

The Cloud Security Alliance (CSA) – a non-profit organization launched in 2009 - is the world's leading organization dedicated to defining and raising awareness to best practices for cloud computing environments. The CSA's activities, knowledge, and extensive network, along with its subject matter expertise, benefit the entire community relaying on and impacted by the cloud through providing a forum by which diverse parties can work together to create and maintain a trusted and safe cloud ecosystem.

BlueBee is ISO 13485:2016 Certified

BlueBee obtained ISO 13485:2016 certification by successfully completing the conformity assessment procedure executed by the independent certification body, BSI. Activities covered by the certification include the design and development of custom-made software solutions and data processing algorithms, intended for use in diagnostics and clinical reporting. Certification by this internationally recognized standard for medical device quality management, demonstrates BlueBee's commitment to providing quality risk-based software development, regulatory compliance and quality management.

BlueBee has constructed and effectively implemented a Quality Management System (QMS) in conformance with the ISO 13485:2016 standard and FDA 21 CFR chapter 820. The QMS incorporates fundamentals of several other standards, such as ISO 14971:2019 and IEC 62304:2006/A1:2015, to ensure requirements are met for regulatory purposes. This service offering may be leveraged by BlueBee's customers, i.e. clinical laboratories and assay kit providers, to meet their own quality assurance requirements and therefore forms a solid base in the path towards obtaining CE IVD (*in vitro* diagnostic) medical device labeling.

ISO 13485:2016 is an international quality management standard for medical devices that specifies requirements for a Quality Management System (QMS) where an organization needs to demonstrate its ability to provide (*in vitro* diagnostic) medical devices and related services that consistently meet customer and applicable regulatory requirements.

When leveraging BlueBee's ISO 13485:2016 QMS for the design and development of Web Applications, BlueBee service offering incorporates requirements from:

- ISO 14971:2019 (Medical devices – Application of risk management to medical devices)

- IEC 62304:2006/A1:2015 (Medical device software – Software life cycle processes)

- *In vitro* diagnostic (IVD) medical device legislation (IVD Directive 98/79/EC and IVD Regulation EU 2017/746)

BlueBee Compliance

BlueBee is committed to demonstrating its compliance with applicable data protection and security regulations and requirements. BlueBee has, therefore, implemented security guidelines and controls to maintain the confidentiality, integrity and availability of its operations.

The following table demonstrates BlueBee's compliance with applicable data protection and security regulations and requirements.

Regulation/Requirements	Description
General Data Protection Regulation 2016/679 (GDPR, EU)	EU regulation on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).
Health Insurance Portability and Accountability Act (HIPAA, USA)	A regulation governing the processing of protected health information (patient data) in the United States of America.
Data Security and Protection Toolkit (DSPT, UK)	Information governance standards (including data protection laws as under the Data Protection Act 1998) applicable to health data in the UK.
Personal Health Information Protection Act 2004 (PHIPA, Ontario, Canada)	Data protection rules regulating the collection, use and disclosure of personal health information in Ontario, Canada.
Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)	Canadian federal legislation governing the collection, use and disclosure of personal information by organisations in the course of commercial activity.
Cyber Security Law (CSL, People's Republic of China)	Chinese law that was enacted to increase data protection, data localization, and cybersecurity in the interest of national security within the People's Republic of China.

BlueBee Complies With Health Insurance Portability And Accountability Act (HIPAA, USA)

BlueBee has put in place all of the necessary measures to comply with the administrative and technical controls required by HIPAA, and maintains policies and procedures to this effect.

Note: *HIPAA governs the privacy and security of protected health information (PHI)[1]. It consists of a set of standards that provide prescriptive guidance for securing and protecting PHI. The US Department of Health and Human Services Office for Civil Rights (HHS-OCR) oversees HIPAA enforcement and compliance.*

HIPAA largely applies to hospitals, healthcare providers, and insurance companies, which are known as Covered Entities under HIPAA. HIPAA also identifies institutions which provide services to Covered Entities, such as software, publishing companies and IT vendors. These are known as Business Associates.

HIPAA consists of 4 rules:

- HIPAA Security Rule
- HIPAA Privacy Rule
- HIPAA Enforcement Rule
- HIPAA Breach Notification Rule

In considering whether it is a business associate, BlueBee ensures that its platform and services do not include any identifiers that would make information it holds PHI. The HHS (U.S. Department of Health & Human Services) has considered whether genetic information is subject to HIPAA, and while such information is health information, it must also be "individually identifiable and maintained by a covered entity" to be classed as PHI.[2]

It should be noted that use of the BlueBee Genomics Platform would not constitute a situation where BlueBee or any other party could identify an individual. Moreover, the information that is received from customers is not considered PHI, and BlueBee is not a business associate. Nevertheless, BlueBee has established its own Business Associate Agreement for use with customers, if needed.

BlueBee Meets Data Security and Protection Toolkit (DSPT, UK) Requirements

Any organisation that accesses United Kingdom's National Health Service (NHS) patient data or national systems, must provide assurances that they are practising good information governance and they must use the Data Security and Protection Toolkit (DSPT) to evidence this by the publication of annual assessments.

Launched by NHS Digital in May 2018, the DSPT replaces the Information Governance Toolkit (IGT) and must be completed annually to provide assurance that organisations adhere to good data security practices. DSPT also supports other recognised data security best practices, including Cyber Essentials Plus and ISO/IEC 27001 – and takes these into account in terms of its requirements on organisations.

The online assessment tool measures and publishes organisations' performance against the National Data Guardian's ten data security standards and relevant elements of GDPR. BlueBee publishes their assessments every year before the end of March. BlueBee – as a company3 – provides services that support the establishment providing care to patients. As a result, BlueBee has met the obligations of the current version of the DSPT standard 2019-20 – version 2.

BlueBee Complies With Personal Health Information Protection Act (PHIPA, Ontario, Canada)

The protection of personal health information is governed provincially in Canada. In the province of Ontario, this is known as the Personal Health Information Protection Act 2004 (PHIPA).

PHIPA governs the collection, use and disclosure of personal health information (PHI) which applies to health information custodians (hospitals, healthcare practitioners, pharmacies) and agents of health information custodians.

In relation to the above-mentioned roles and responsibilities, under PHIPA, BlueBee is classified as an agent, as it processes genetic data on behalf of and solely on authorisation from the health information custodian, i.e. BlueBee's customer.

The Information Privacy Commissioner of Ontario has issued Privacy Impact Assessment Guidelines for PHIPA allowing health information custodians to review the impact a proposed information system, technology or program, may have on the privacy of an individual's personal health information under PHIPA. As a health information custodian, BlueBee decided to document, via the privacy impact assessment questionnaire, how it meets certain requirements in order to help potential customers in assessing its offering – this is available upon request.

BlueBee Complies With Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)

In Canada, the protection of personal information is regulated by the Personal Information Protection and Electronic Documents Act 2000 (PIPEDA).

Compliance with PIPEDA is overseen by the Office of the Privacy Commissioner of Canada (OPC). Compliance with this act involves adherence to PIPEDA's reasonable safeguards. With experience in implementing a well-functioning information security management system from its ISO/IEC 27001:2013 certification, BlueBee leveraged the policies and procedures already implemented in order to ensure compliance with PIPEDA guidelines.

The reasonable safeguards include: Risk Management, Security Policies, Human Resources Security, Records Management, Access Control, Technical Security, Physical Security, Operating Systems, Network Security, Information Systems, Acquisition, Development, Maintenance, Incident Management Business Continuity Planning and Compliance.

PIPEDA further stipulates 10 principles for fair information practices, concerning the collection, use, disclosure of and providing access to personal information. These include accountability, identifying purposes, consent, limiting collection, limiting use, disclosure, and retention, accuracy, safeguards, openness, individual access and challenging compliance. These principles have been incorporated into the PIPEDA Diagnostic Checklist to which BlueBee closely adheres.

BlueBee Complies With General Data Protection Regulation (GDPR, EU)

Processing large volumes of personal data in a cloud environment requires additional safeguards under the data protection law. BlueBee complies with the requirements of the GDPR and the specific requirements that apply to the processing of personal health data in a cloud environment.

BlueBee's internal standards ensure compliance within all applicable member states.

Note: *As of May 25, 2018, Directive 95/46/EC was replaced by a regulation commonly known as the General Data Protection Regulation (GDPR). Contrary to a directive, a regulation has a direct effect and enforces a single global legislation set. However, the GDPR does allow member states to provide stricter rules for personal health data and therefore small differences between member states may still arise.*

BlueBee is committed to complying with the GDPR and has updated its organization, its processes, and its contractual framework as required.

Basic Principles Of The EU Data Protection Law

BlueBee assumes that the data being processed by means of its cloud-based platform is personal data[4] processed by automatic means. Consequently, the rules applicable to the processing of personal data by non-automatic means are not explained in this white paper.

Note: *The GDPR applies to the processing of personal data wholly or partly by automatic means by a controller located in an EU member state.*

For the purposes of applying the GDPR, a distinction must be made between the controller and the processor[5]. This distinction is important because it serves to attribute accountability and liability for data processing operations.

Controller
- The entity which alone or jointly with others determines the purposes and means of processing personal data.
- Responsible for ensuring that data processing operations comply with data protection principles, such as lawfulness and fairness, purpose limitation, adequacy, accuracy, data retention, etc.

Processor
- The entity that processes personal data on behalf of the data controller, typically a service provider.

Because BlueBee's activities consist of hosting and providing access to a cloud-based analysis platform, BlueBee's activities are essentially those of a processor, i.e. its platform serves to process personal data on behalf of its client. As such, BlueBee's clients are responsible for ensuring that the data processing operations comply with data protection principles. For this reason, BlueBee requests a written assurance from its clients that they are legally entitled to process the personal data entrusted to BlueBee. BlueBee, as a processor, can only assume liability for the processing that takes place within the perimeter of its liability.

This also implies, that when BlueBee processes data from physical persons or employee data from clients (e.g. for contract management purposes), then BlueBee is the controller for this data processing activity. The purpose is client management. In this instance, BlueBee – as a data controller – complies with the data protection principles.

Both activities are adequately described in and governed by BlueBee's terms and conditions and privacy statements.

Contractual Requirements Between BlueBee And The Client

GDPR does impose some obligations on the controller and the processor in relation to the appointment of data processors. These obligations are reflected in BlueBee's terms and conditions.

First, controllers may only appoint processors that offer sufficient guarantees with respect to compliance with the GDPR.

To this effect, BlueBee has invested substantial cost and effort to ensure that compliance with these requirements can be demonstrated, by achieving the ISO/IEC 27001 certification, among others. In doing so, BlueBee offers its clients a cost-

effective alternative to data protection audits. Data protection authorities accept that certification is a valid alternative to data protection audits in the context of large-scale public cloud computing services.

Second, the processing of personal data by a processor must be governed by a contract or a legal act binding the processor to the controller. It must also stipulate that the processor, i.e. BlueBee, may only act on documented instructions of the controller (the client using the cloud-based platform), as well as impose the requisite security obligations and various other requirements. Here BlueBee's terms and conditions impose a clear obligation on BlueBee to implement and maintain the required adequate security obligations and to process personal data solely in accordance with the documented instructions of the client (controller).

BlueBee's terms and conditions also include all legally required obligations and wording pursuant to article 28 of the GDPR. The GDPR only legally accepts the data processing agreement in writing, including in electronic form. By entering into a written data processing agreement with BlueBee and by using BlueBee's terms and conditions, the client can rest assured that she/he complies with his obligations as a controller in relation to the appointment of a reliable processor.

BlueBee Complies With Cyber Security Law (People's Republic of China)

On 7 November 2016, the Cyber Security Law (CSL) was issued and it took effect on 1 June 2017. The official implementation of the CSL marks the gradual formation of China's new legal framework for cybersecurity and data protection. Among other things, the CSL covers the following aspects:

- personal information protection;
- general network protection obligations of the network operators and the multi-level protection scheme (MLPS);
- enhanced protection for the critical information infrastructure (CII);
- data localisation and security assessment for the cross-border transfer of personal information and important data;
- security review of the network products and services.

As the CSL is a high-level law and does not provide practical guidelines, China has been drafting a series of related implementation regulations and national standards. These implementation regulations and national standards, together with the CSL, constitute China's legal regime for cybersecurity and data protection.

On June 13, 2019, the Cyberspace Administration of China (CAC) released a draft regulation governing the transfer of personal information out of China: "Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment)". The draft regulation formulates measures to ensure the security of personal information during cross-border data flows, are in accordance with the CSL and other relevant laws and regulations.

Network Operators who provide Personal Information6 (PI) collected in the course of operations within the mainland territory of the People's Republic of China, shall conduct security assessments in accordance with these Measures. If it is determined by the security assessment that the outbound transfer of personal information may affect national security or harm the public interest, or that the security of personal information is difficult to effectively protect, such information shall not leave the country.

BlueBee, as a provider of cloud computing services that process users' Personal Information and patient's Personal Sensitive Information[7] (PSI), has conducted this security assessment. We concluded that both PI and PSI of Chinese citizens, may not leave the mainland territory of the People's Republic of China. Our conclusion is based on the fact that BlueBee is considered a provider of Critical Information Infrastructure[8] (CII) because we manage cloud services for scientific research and for healthcare purposes (both critical industries). BlueBee has extended data operations to Mainland China to serve genomic data processing needs in compliance with China's new legal framework for cybersecurity and data protection.

BlueBee Platform Runs On Highly Secured Physical Cloud Infrastructure

Running the BlueBee Genomics Platform on a high-performance private cloud infrastructure allows BlueBee to take advantage of the broad spectrum of built-in state-of-the-art features that ensure compliance, privacy, and security. The cloud infrastructure works with independent auditors and third-party physical cloud infrastructure providers to meet the industry's most stringent compliance needs. Compliance Standards implemented at these physical cloud infrastructure providers include: SOC Reports, ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 certifications, HIPAA Compliance, and GDPR Compliance.

This guarantees a solid foundation on which the BlueBee Genomics Platform is built.

BlueBee Guarantees Ongoing Platform Monitoring To Combat All Risks and Threats

Security is not just about building a secure and stable infrastructure; it includes maintaining and monitoring the platform against all risks and threats. To ensure that the BlueBee Genomics Platform is secure and fully functional at all times, the BlueBee team follows Best Practices guidelines and:

• Guarantees ongoing infrastructure and platform vulnerability assessments,

• Employs ongoing performance testing mimicking clients' analyses workflows,

• Conducts regular random log reviews and system-level inspections to identify any suspicious behavior so that it can take immediate and necessary actions.

References

1   PHI refers to individually identifiable information, such as name, contact details, biometric data, health plan information, geographical information, social security and medical record numbers.

2   See, HHS FAQ, dated 20 Feb 2002, https://www.hhs.gov/hipaa/for-professionals/faq/354/does-hipaa-protect-genetic-information/index.html

3   "An organisation external to the NHS, contracting with an NHS establishment to provide non-healthcare goods, services that support the establishment providing care to patients." – https://www.dsptoolkit.nhs.uk/Help/Attachment/235

4   This will not always be the case, as the genetic data may also relate to plants, animals, bacteria.

5   For more information: Article 29 Data Protection Working Party, Opinion 1/2010 of 16 February 2010 on the concepts of "controller" and "processor".

6   Personal Information (PI): "Refers to various information recorded by electronic or other means that, alone or in combination with other information, can identify a natural person's personal identity, including but not limited to the name of the natural person, date of birth, ID number, personal biometric information, address, phone number, etc." – Article 21 of the Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment).

7   Personal Sensitive Information (PSI): "Refers to personal information that, if leaked, stolen, tampered with, or illegally used, may endanger personal and property safety, or cause damage to a person's reputation and physical and/or mental health. – Article 21 of the Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment).

8   Critical Information Infrastructure (CII): "Refers to network infrastructure and information systems operated or managed by work units (incl. providing Cloud computing), which whenever destroyed, cease functioning or leak data may gravely harm national security, the national economy, the people's livelihood and the public interest." – Article 18 of the "Critical Information Infrastructure Security Protection Regulations (Opinion seeking Draft).

Legal Notices

BlueBee © 2020. All Rights Reserved.

The recipient is authorized to copy or reproduce this document within his own organization as may be reasonably necessary for the purpose of evaluating BlueBee's proposal. Any such copy or reproduction will include all notices set out on this page.

Trademarks

BlueBee and BlueBee Genome Analysis Platform are trademarks of BlueBee Holding BV, registered office Laan van Zuid Hoorn 57, 2289 DC Rijswijk, The Netherlands.

Important

This document is supplied for information purposes only and shall not be binding nor shall it be construed as constituting any obligation, representation or warranty on the part of BlueBee. Although BlueBee has taken great care to provide accurate, complete and current information, BlueBee does not guarantee that this white paper is free from errors.

The information in this document is the latest available at the date of its production and may change from time to time. Note in particular that BlueBee services and products evolve over time. If you need to check whether the information in this document is still valid, please contact BlueBee.

About BlueBee

BlueBee is a rapidly configurable genomics data analysis solutions provider enhancing the value of genomic technologies and services. BlueBee enables our partners to globally scale by delivering a production-ready, robust infrastructure that is compliant with local requirements for clinical data applications and user-centric so that together, we can accelerate new discoveries and advance precision medicine.

BlueBee