WHITE PAPER

BLUEBEE DATA SECURITY & COMPLIANCE

Data security and protection are of utmost importance in our digital age, especially with new and complex technologies that include server, cloud, and internet technologies.

BLUEBEE
High Performance Genomics

ERKELENS
LAW

TABLE OF CONTENTS

OVERVIEW

This is particularly relevant in the context of human genomics data processed for clinical and research purposes. Additional, independent complexities exist due to local data privacy and regulatory compliance requirements.

Bluebee and its Genomics Platform – with its data center partners – is compliant with all applicable local and global regulations and standards. This guarantees customers state-of-the-art data security as well as regulatory compliance. The combination of sophisticated data center infrastructure with the Bluebee Genomics Platform and certified compliance allows Bluebee to meet the demanding requirements of customers who work with patient-derived, sensitive sequence data, which requires the most stringent security controls.

COMPLIANCE WITH DATA PROTECTION AND SECURITY REQUIREMENTS

This document details how Bluebee ensures its clients compliance with data protection and security requirements when using the Bluebee cloud-based accelerated genomics analysis platform to enable fast, efficient, and affordable processing of large volumes of clinical sequence data.

This document is divided into four sections:

1. An overview of the security measures implemented for Bluebee's cloud-based accelerated genomics analysis platform.
2. An overview of the mechanisms in place that ensure guaranteed availability while addressing specific cloud processing requirements.
3. An overview of Bluebee's security and privacy certificates implemented with regard to its cloud-based accelerated genomics analysis platform.
4. A summary of the measures taken to ensure that Bluebee's clients can reliably use the cloud-based accelerated genomics analysis platform in a manner which is compliant with applicable data protection legislation.

BLUEBEE'S GENOMICS PLATFORM SECURITY MEASURES

Extensive security measures ensure the highest level of security of sensitive human genomics data. The Bluebee 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 integrity of the data flowing across the entire platform whether processed in the cloud, transferred via the internet, or stored at rest. Simply speaking the platform has been designed with confidential patient information and multi-layered data security in mind. This ensures an environment that covers the strictest of security controls.

The Bluebee Platform is deployed on a private cloud. In addition, the Bluebee platform runs on private bare metal servers ensuring the highest degree of isolation, which is also typically a pre-requisite for High Performance Computing. On top of the physical aspect, the analytical 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 superior platform and infrastructure security without compromising performance as compared to the use of a Virtual Private Cloud. Furthermore, this combination offers virtually unlimited scaling for sequence data analysis and storage.

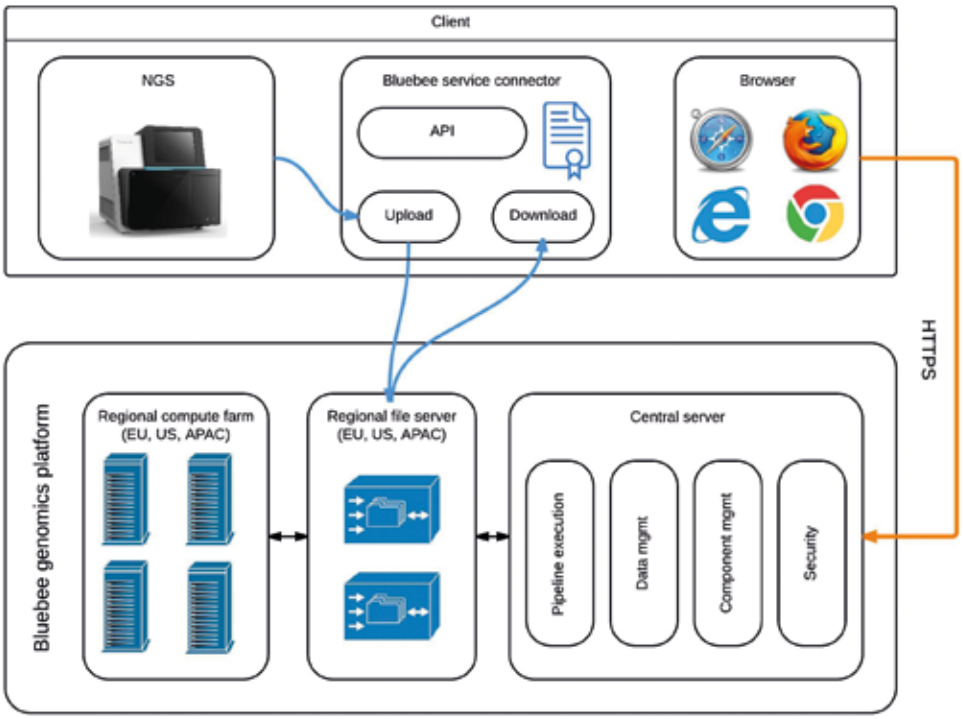

FIGURE 1: BLUEBEE GENOMICS PLATFORM BUILDING BLOCKS OVERVIEW.

BLUEBEE'S DATA SECURITY LEVELS

Below are the multiple security features embedded within the Bluebee Genomics Platform.

SECURITY FEATURES	BLUEBEE GENOMICS PLATFORM	ADVANTAGES
Two factor authentication	Step authentication for sensitive actions*.	Ensures highest level confidentiality
Login policies	Enforces strong password, renewal period, and inactivity timeout.	Ensures highest level confidentiality
Anonymization	Store patient data alongside data files. Use patient data throughout the processing chain or provide only a reference link back to the patient 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. Object** owner, via owner privileges, controls finegrained access to object for other users, companies, and communities.	Ensures fine-grained access privileges
Audit trailing	All actions for all objects within the platform are recorded (includes viewing an object).	Assures regulatory requirements are met
Four eyes control	Applies to sensitive actions* on shared data and access-granting to permitted data**. Sensitive actions at all times must be approved by another user with appropriate access permissions. Combines with step-up authentication.	Protects sensitive data and actions

SECURITY FEATURES	BLUEBEE GENOMICS PLATFORM	ADVANTAGES
Role based access	Fine-grained security controls of who can do what within the platform – applies to all objects**. A complex matrix allows the clients' administrators to setup granular security definitions to fit organizational requirements.	Allows an administrator to implement organizational control requirements
PKI infrastructure	A framework that provides the generation, production, distribution, control, accounting and destruction of public key certificates. Integrates digital certificates, public-key cryptography, and Certification Authorities into an enterprise-wide network security architecture.	Provides digital signature and encryption capabilities Ensures the origin and integrity of the data** flowing across the entire platform Assures 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 defined appropriate actions will be taken.	Ensures data privacy when transferred over the internet, processed in the cloud, and stored at rest

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

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

COMPREHENSIVE PLATFORM SECURITY ARCHITECTURE

Bluebee's high performance genome analysis platform is an industrial-level secure and private cloud solution that supports high performance and highly scalable sequence data processing and storage for an individual or an enterprise organization in the clinical, pharmaceutical, and research domain.

Key capabilities:

1. Direct and secure integration with sequencer instrumentation and infrastructure for transparent and efficient data upload and processing of sequence data within a diagnostics workflow.
2. Highly configurable, flexible, and extensible sequence data analysis pipelines for bioinformaticians to run version controlled sequence data analyses.
3. On-demand scalable sequence data analysis via parallel processing of analysis pipelines which support data analysis surges when needed.
4. Feedback-loop based job monitoring and job prioritization which allow quick adjustments to clinical requirements and research findings.
5. Instantaneous delivery of interpretation findings for expedited insights gathering.

The capabilities associated with the provided analytics pipelines 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 applies:

1. The Bluebee Genomics Platform runs on private bare metal servers with the highest degree of isolation, as the machines are exclusively used by Bluebee.
2. The Bluebee analysis pipelines are executed in a container ensuring they stay within the boundaries that are set out by the platform; this includes access to data and resource consumption.
3. The Bluebee private cloud operates in multiple geographic regions and provides users with elaborate functionality for audit trails, encryption, data storage and retrieval.

The above listed three elements allow Bluebee to deliver superior platform and infrastructure security without compromising performance compared to the use of a Virtual Private Cloud. Furthermore, this combination offers virtually unlimited scaling for data analysis and storage.
The primary security consideration for Bluebee is that only authorized users can access their safely contained and isolated data.

31 GLOBAL DATA CENTER DEPLOYMENTS

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

FIGURE 2 : TRULY GLOBAL DEPLOYMENT IN REGIONAL DATACENTERS

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

This distributed model allows the Bluebee platform to store the data and perform computational analysis within a location close to the source of the data and 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 thirty-one data centers in twenty-two worldwide locations currently supported.

EUROPE	AMERICAS	ASIA PACIFIC
Amsterdam, The Netherlands	Dallas, TX, USA	Chennai, India
Frankfurt, Germany	Houston, TX, USA	Hong Kong, China
London, England	San Jose, CA, USA	Singapore, Singapore
Milan, Italy	Sao Paulo, Brazil	Sydney, Australia
Oslo, Norway	Seattle, WA, USA	Melbourne, Australia
Paris, France	Washington DC, VA, USA	Tokyo, Japan
	Montreal, Canada Seoul, South Korea	Seoul, South Korea
	Toronto, Canada	
	Querétaro, Mexico	

The Data Residency Control feature allows users to have one 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 one can still securely collaborate on and share the data.

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 its customers who need to process genomics data in a compliant, secure, and reliable manner.

When processing genomic data, the data processing infrastructure must always be available and highly secured. For this reason, Bluebee carefully selects reliable data center partners that provide guarantees in terms of high-level availability. Furthermore, Bluebee actively ensures that its platform can operate within those data centers in accordance with high-level security requirements.

> *Note: Identified specific risks in the context of the use of cloud computing services are based on a public cloud infrastructure which resulted in specific guidance from the Article 29 Data Protection Working Party, a European advisory board created under the Directive 1995/46/EC[1], as well as data protection authorities of EU member states.*

The 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 origin and integrity of the data flowing 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 3rd party
Portability	Standardized tools for data output	No vendor lock-in with no legal impediments to export 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 developed a business continuity and a disaster recovery plan for its business processes. The Bluebee Genomics Platform is supported by Bluebee's business continuity and disaster recovery plan. The platform is installed on a high available private cloud infrastructure in ISO 27001:2013 certified facilities, which are built following the Uptime Institute's Tier III standard design.

Data security and redundancy is protected by Bluebee's proprietary failover application 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 (30km distance).

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

INTEGRITY

Given the nature of the data, e.g. sensitive human genetics data, their integrity are of 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. The service description provides additional details on how Bluebee helps its clients to process their data in a reliable manner, thereby ensuring data integrity.

> *Note: Article 29 Data Protection Working Party defines integrity as "the property that data is authentic and has not been maliciously or accidentally altered during processing, storage, or transmission".*

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 the Bluebee cloud environment, the data is encrypted both "in transit" and "at rest".

BLUEBEE DATA ENCRYPTION	
In transit	TLS
At rest	AES256
Cold storage	AES128

Specifically, Bluebee has implemented a mechanism whereby all personal data that is being processed within the Bluebee Genomics Platform is being encrypted.

In addition to data encryption, Bluebee has implemented the necessary access controls to limit access to its platform. Given the purpose of Bluebee's 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, confidentiality is further ensured by means of identity and access management, using strong authentication mechanisms. It is also suggested that data processors' employees and contractors must be bound by confidentiality obligations.

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

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

TRANSPARENCY

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

> *Note: The Article 29 Data Protection Working Party has identified particular requirements in relation to transparency, where required for a fair processing. As such, the Article 29 Data Protection Working Party requires that the data controller is informed about the location of the datacenters used to provide the services.*

ISOLATION (PURPOSE LIMITATION)

The specifics of a public cloud infrastructure pose additional risks in relation to the data that is being processed on this infrastructure, notably due to the same physical hardware being used for several clients (e.g. memory and storage). Data protection authorities perceive this situation as a risk in terms of 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 a reinforced application of the need-to-know principle, enforced through technical and organizational measures (including access limitation and role-based access). It also includes measures that ensure data segregation, for instance by containerizing the data that is being stored.

To ensure data is not accidentally disclosed to other parties as a result of the processing activities on the Bluebee Genomics Platform, Bluebee's platform follows industry standard data segregation techniques. Furthermore, Bluebee's cloud-based platform restricts access to the cloud-based platform 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 functionalities are included in the platform. For more details, see the section "Bluebee's Data Security Levels" above.

PORTABILITY AND EXIT-MANAGEMENT

A particular focus of the data protection authorities relates to 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 a situation of vendor lock-in.

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. 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's terms and conditions clearly stipulate that the client remains 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 itself to destroying client data at the end of an agreement in accordance with applicable industry standards. This obligation also serves to increase the confidentiality of the 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.

> *Note: The Article 29 Data Protection Working Party describes IT accountability as "the ability to establish what an entity did at a certain point in time in the past and how".*

INTERNATIONAL DATA TRANSFERS AND DATA RESIDENCY REQUIREMENTS

Since Bluebee is based in the European Economic Area and its datacenters are also located in the European Economic Area, the restrictions on international data transfers do not apply when personal data are being processed by means of the Bluebee genomics platform. Therefore, the EU presence of Bluebee is a substantial regulatory and practical advantage, even though international data transfers can validly be organized under the Directive 95/46/EC. While the current legal framework for data transfers to the US (the so-called EU/US Privacy Shield) is mired by legal uncertainty[2], the same applies to some extent for the current versions of the standard contractual clauses and BCR[3]. Even if standard contractual clauses would be used to transfer personal data to third countries, additional formalities may apply[4].

> *Note: Data protection requirements do not impede the use of cloud services with the European Economic Area due to the fact that the Directive 95/46/EC 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 pre-approved EC standard contractual clauses.*
>
> *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 law.*

Bluebee's platform is generally capable of being deployed in datacenters located in the same country as the data controller's establishment, as detailed in section 3.3. Bluebee's cloud based genomics platform can therefore comply with these additional legal and regulatory restrictions which imposes the processing and storage of such data in the member state of the data controller.

BLUEBEE CERTIFICATIONS

CERTIFICATION

Bluebee is committed to demonstrating its compliance with applicable data protection and security requirements. Bluebee has therefore implemented security guidelines and controls to maintain confidentiality, integrity and availability of Bluebee's operations. Furthermore, Bluebee's data protection and security controls have been successfully audited against various international and recognized standards, including ISO 27001:2013.

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

STANDARD/REGULATION	DESCRIPTION	BLUEBEE GENOMICS PLATFORM
ISO 27001:2013	International standard on the establishment, implementation, maintenance, and continuous improvement of information security management systems.	✔
HIPAA	A regulation governing the processing of protected health information (patient data) in the US.	✔
Information Governance Toolkit (NHS, UK)	Information governance standards (including data protection laws as under Data Protection Act 1998) applicable for the treatment of health data in the UK.	✔
Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)	A detailed compilation of global industry based standards for cloud service providers	✔
Personal Health Information Protection Act 2004 (PHIPA)	Data protection rules regulating the collection, use and disclosure of personal health information in Ontario, Canada.	✔
Personal Information Protection and Electronic Documents Act 2000 (PIPEDA)	Canadian federal legislation governing the collection, use and disclosure of personal information by organisations in the course of a commercial activity.	✔
NEN 7510:2011	Information security management in healthcare standard applied in the Netherlands.	✔
EU Data Protection Directive (Directive 95/46/EC)	Data protection rules governing the use of personal data in the EU.	✔

Note: The Article 29 Data Protection Working Party acknowledges and accepts that independent verification and/or certification by a reputable third party can be a credible alternative to data protection audits undertaken by data controllers, provided that the cloud service provider's data protection controls have been audited against a recognized standard. In taking up this position, the Article 29 Data Protection Working Party agrees that auditing a multi-party public cloud infrastructure is technically and/or logistically impossible or undesirable in view of the technical and practical risks this may pose.

Bluebee is confident that this certification may be presented in lieu of individual assessments by data controllers. By offering this possibility, Bluebee reduces the administrative and financial burden for its clients to achieve data protection compliance when appointing data processors.

BLUEBEE IS ISO 27001:2013 CERTIFIED

Bluebee has been ISO 27001: 2013 certified by an independent auditor for the full scope of its activities which includes development, management, and support of a cloud-based genomics analysis platform for processing of large volumes of sequence data.

In compliance with the ISO 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 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 27002 consists of best practices which support and contribute to ISO 27001 compliance.

BLUEBEE COMPLIES WITH HEALTH INSURANCE PORTABILITY ACT (HIPAA)

Bluebee has put in place all 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)[5]. 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, 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*

It is necessary to comply with the standards in each rule to be HIPAA compliant.

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.[6]

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 will not be 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 INFORMATION GOVERNANCE TOOLKIT

Bluebee has met the obligations of the current version of the Information Governance Toolkit – version 14, valid until March 2018 – and complies with the Information Governance Assurance Statement. This has been deemed satisfactory by NHS Digital.

The Information Governance Statement of Compliance (IG SoC) is the process in the United Kingdom by which organisations enter into an agreement with the Health and Social Care Information Centre (HSCIC). IG SoC is governed by the National Health Service (NHS). The process includes compliance with the Information Governance Toolkit, a portal through which organisations evidence how they meet a range on security related requirements, such as information governance, information security assurance, and confidentiality and data protection assurance.

The NHS has categorised organisations conforming with the Information Governance Toolkit according to their activities. In line with this, Bluebee is considered as a Commercial Third Party.[7]

BLUEBEE HAS ACHIEVED LEVEL ONE CSA STAR ASSESSMENT

Bluebee have achieved Level One CSA STAR Assessment which demonstrates our ongoing commitment to platform and data security. In compliance with Level One CSA STAR Assessment Bluebee customers can be assured that the highest level of cloud security is in place addressing different security aspects.

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 of best practices to help ensure a secure cloud computing environment. CSA's activities, knowledge, and extensive network with its subject matter expertise benefit the entire community relaying on and impacted by the cloud and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

BLUEBEE COMPLIES WITH PERSONAL HEALTH INFORMATION PROTECTION ACT (PHIPA)

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

PHIPA governs the collection, use and disclosure of personal health information (PHI) and 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 will be classed 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 a 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 an agent of 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 on request.

BLUEBEE COMPLIES WITH PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

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). The compliance involves adherence to the PIPEDA reasonable safeguards. With experience in implementing a good functioning information security management system from its ISO 27001:2013 certification, Bluebee leveraged the policies and procedures implemented to ensure compliance with PIPEDA guidance.

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 of 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 in the PIPEDA Diagnostic Checklist which Bluebee has documented to demonstrated how it adheres to the abovementioned principles.

BLUEBEE IS NEN 7510:2011 CERTIFIED

NEN 7510:2011 is the Dutch standard on information security for organisations handling patient data. The standard is combined of ISO 27001, ISO 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 7510:2011 emphasise Bluebee's commitment to security in particular with regard to patient data and its consideration for local regulatory compliance requirements.

NEN 7510:2011 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 7510:2011 certification mirrors the scope of its ISO 27001:2013: "Develop, manage, support a cloud based genomics platform processing of large volumes of data", and certification is valid for 3 years with annual surveillance assessments.

Note: All of the abovementioned standards and certifications are reviewed annually.

BLUEBEE IS COMPLIANT WITH THE DIRECTIVE 95/46/EC AND PERSONAL HEALTH DATA

Processing large volumes of personal data in a cloud environment requires additional safeguards under data protection law. Bluebee complies with, and even exceeds, the requirements of the Directive 95/46/EC and the specific requirements that apply to the processing of personal health data in a cloud environment.

BLUEBEE ENSURES COMPLIANCE WITH ALL APPLICABLE EU MEMBER STATES LOCAL LEGISLATION

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

Note: The European Union has an established history of privacy and data protection that is currently regulated by the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. The directive includes protection of individuals regarding the processing of personal data and the free movement of such data ("Directive 95/46/EC").

Directives do not apply directly in local member states, but must be implemented in local member state legislation. This implies that each EU member state currently has local legislation which reflects the Directive 95/46/EC [8]. Therefore, small differences between member states exist.

The Directive 95/46/EC will be replaced by a regulation beginning May 25, 2018 [9]. This regulation is commonly known as the General Data Protection Regulation (GDPR). Contrary to a directive, a regulation has direct effect and enforces a single legislation set.

Bluebee is committed to complying with the GDPR and will update its organization, its processes, and its contractual framework as required. Future versions of this white paper will reflect such changes.

BASIC PRINCIPLES OF EU DATA PROTECTION LAW

Bluebee assumes that the data being processed by means of its cloud-based platform is personal data [10] 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 Directive 95/46/EC applies to the processing of personal data wholly or partly by automatic means by a data controller located in an EU member state.*

For the purposes of applying the Directive 1995/46/EC, a distinction must be made between the data controller and the data processor [11]. This distinction is important because it serves to attribute accountability and liability for data processing operations.

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

Because Bluebee's activities consist of hosting and providing access to a cloud-based genomics platform, Bluebee's activities are essentially those of a data processor, i.e. its platform serves to process personal data on behalf of its client. As such, Bluebee's clients are responsible for determining that the data processing operation complies with the data protection principles. For this reason, Bluebee requests a written assurance from its clients that its clients are legally entitled to process the personal data entrusted to Bluebee. Bluebee, as a data 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 clients who are physical persons or employee data from clients (e.g. for contract management purposes), then Bluebee is the data 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.

CONTRACTUAL REQUIREMENTS BETWEEN BLUEBEE AND THE CLIENT

If abstraction is made of the legal requirements in relation to confidentiality of processing, the Directive 95/46/EC does not impose direct obligations on a data processor. The Directive 1995/46/EC does however impose some obligations on the data controller in relation to the appointment of data processors. These obligations are reflected in Bluebee's terms and conditions.

First, data controllers may only appoint data processors that offer sufficient guarantees in respect of the technical measures and organizational security measures. These measures must protect the personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Bluebee has implemented robust technical and organizational security measures that enable its customers to comply with this obligation in relation to the appointment of data processors.

Moreover, a data controller must be able to demonstrate compliance with these security requirements. To that effect, Bluebee has invested substantial cost and effort to ensure that compliance with these requirements can be demonstrated, amongst other by achieving ISO 27001 certification. In doing so, Bluebee offers its clients a cost-efficient 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 data processor must be governed by a contract or a legal act binding the data processor to the data controller. It must also stipulate that the data processor, i.e. Bluebee, may only act on instructions of the data controller (the client using the cloud-based platform), as well as impose the requisite security obligations. 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 instructions of the client (data controller).

The Directive 95/46/EC legally accepts the data processing agreement in writing or in another equivalent (i.e. electronic, click-wrap mechanism) form.

By using Bluebee's terms and conditions, the client can be assured that he complies with his obligations as a data controller in relation to the appointment of a reliable data processor.

BLUEBEE PLATFORM RUNS ON HIGHLY SECURED CLOUD INFRASTRUCTURE

Running the Bluebee Genomics Platform on the SoftLayer high performing 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 internal SoftLayer compliance department works with independent auditors and third-party organizations to meet the industry's most stringent compliance needs. The series of SoftLayer Compliance Standards (http://www.softlayer.com/compliance) includes SOC Reports, ISO 27001, ISO 27017, and ISO 27018 certification, PCI Compliance, HIPAA Compliance, CJIS Standards, and EU Model Clauses. Lastly, SoftLayer is an approved member of the EU-US Privacy Shield Framework.

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 at all times secure and fully functional, 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 to take immediate and necessary actions.

REFERENCES

1 Article 29 Data Protection Working Party, Opinion 05/2012 of 1 July 2012 on Cloud Computing. See also: CNIL, Recommendations pour les entreprises qui envisagent de souscribe à des services de Cloud computing; ICO, Guidance on the use of cloud computing; CPVP, Avis n° 10/2016 du 24 février d'initiative relatif au recours au cloud computing par les responsables du traitement.

2 On 6 October 2015, the Court of Justice of the European Union invalidated the adequacy finding of the European Commission in relation to the Safe Harbor agreement, which enabled the international transfer of personal data to the US (case C-362/14, Maximillian Schrems v Data Protection Commissioner). A new mechanism, the EU/US Privacy Shield, has in the meantime replaced its predecessor, but already Digital Rights Ireland has initiated an action for annulment with the General Court.

3 The German data protection authority for Schleswig-Holstein, for instance, criticized the use of the standard contractual clauses: https://www.datenschutzzentrum.de/artikel/981-.html. Moreover, a case was brought before the Irish High Court in relation to the validity of the standard contractual clauses. It is expected that the question regarding the validity of the standard contractual clauses will be referred to the Court of Justice of the European Union. The European Commission has recently adapted its adequacy decision to anticipate the outcome of this court case.

4 In some countries, such as Belgium, the use of standard contractual clauses does not exempt the data controller of the requirements of prior approval and notification, which may cause additional cost and delays that may be avoided by using the Bluebee platform.

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

6 See, HHS FAQ, dated 12/20/2002, http://www.hhs.gov/hipaa/for professionals/faq/354/does-hipaa-protectgenetic-information/index.html.

7 "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.igt.hscic.gov.uk/resources/User%20Guide-Organisation%20Types.pdf

8 E.g. the French Data Protection Act of 1978, the Belgian Act of 8 December 1992 on privacy protection in relation to the processing of personal data, the Dutch Data Protection Act of 6 July 2000, the German Federal Data Protection Act and the English Data Protection Act 1998.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), often referred to as GDPR.

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

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

Johan Vandendriessche is a partner at Erkelens Law. His practice covers ICT law, data protection and privacy law, as well as intellectual property law.
Johan combines his law practice with several academic activities. He is, amongst others, Visiting Professor in ICT law at the University of Ghent and Visiting Professor in ICT and Data Protection Law at the HoWest University of Applied Science.

ERKELENS LAW

LEGAL NOTICES

CONFIDENTIALITY

This document contains proprietary and confidential information of Bluebee. The recipient should not disclose this document to third parties without the prior written permission of Bluebee.

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.

The Bluebee genomics platform supports cross-functional teams of life science researchers and clinicians by effectively centralizing and managing their genomics data processes and storage needs.

Bluebee accelerates genomics insights discovery via the delivery of optimized data analysis pipelines, employing both supercomputing and private cloud technologies. This results in a unique high performance cloud-based genomic analysis platform that enables efficient and affordable processing, and insight generation from ever-increasing genomic data.

THE NETHERLANDS

Laan van Zuid Hoorn 57
2289 DC, Rijswijk
The Netherlands

UNITED STATES

1 Broadway
Cambridge, MA 02142
United States

CONTACT US

US: +1 844 662 3511
ROW: +31 88 2140 200
info@bluebee.com
www.bluebee.com

SOCIAL MEDIA

@BluebeeGenomics
Bluebee

BLUEBEE
High Performance Genomics

20171120