April 20, 2021

WHITEPAPER:

YOUNiQ Data Protection: Biometric and Cybersecurity Compliance with New York, Illinois and European Data Protection Laws

Contents

LEGAL DISCLAIMER

I. Introduction

Precise Biometrics comes from Sweden, where businesses expect that biometric technology should be designed from start-to-finish for transparent compliance with the European Union's General Data Protection Regulation ("GDPR"). YOUNiQ is the product of GDPR-compliant privacy-by-design, encompassing the seven key principles of the GDPR, including:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These GDPR principles lie at the heart of YOUNiQ's approach.

Similarly, US companies and users should expect biometric security technology that transparently complies with US law. This white paper discusses the nation's leading biometrics law, Illinois' Biometric Information Privacy Act, which makes it unlawful to, among other things, use Illinoisans' biometric image without first informing them in writing, and obtaining their consent. The most comprehensive US cybersecurity law – with broad cross-sector application – is New York State's recently-enacted cybersecurity law, the SHIELD Act, which asserts jurisdiction over anyone who possesses a New Yorker's personal information anywhere in the world. This white paper offers a discussion of the New York SHIELD Act's requirements for reasonable cybersecurity safeguards as may concern businesses' use of YOUNiQ.

Privacy advocates rightly are concerned about facial recognition technologies that – unlike YOUNiQ – harvest people's biometric information from photographs posted on Facebook, other social media sites, and anywhere else they may be posted on the Internet. These controversial Internet-scraping companies amass massive databases of photographs of random men, women and children and compute biometric data for each one. The individuals involuntarily entered into these databases are not asked whether they consent to the use of their likenesses or to be tracked biometrically by the technology going forward.

By contrast, YOUNIQ only collects selfie images provided directly by the individuals who seek to be granted security access though the system. When registering for YOUNiQ on their smartphone, each individual is advised of their data privacy rights and invited to provide their positive consent, which is absolutely required before the person's image is processed into YOUNiQ. All personal data is wiped from storage when the individual is removed from the biometric security system, or consent is revoked.

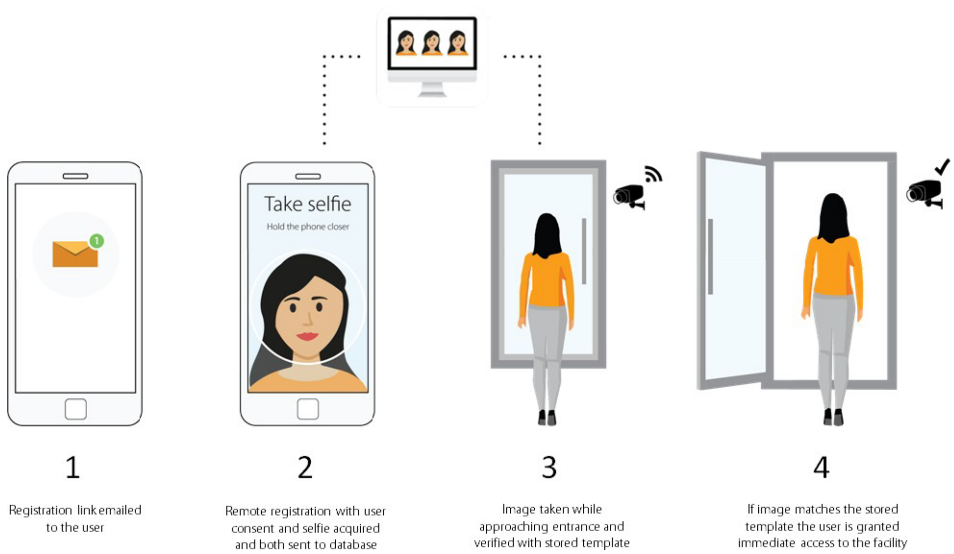
This white paper will summarize how YOUNiQ works, including the proprietary biometric template created from users' selfie images. It then details how user data – including a selfie photo uploaded by the user – is stored in two separate secure repositories. After discussing Illinois' BIPA, it focuses on the SHIELD Act, its terms, and the administrative, technical and physical safeguards it mandates. We consider how YOUNiQ addresses each of those safeguards, and what customers should take into consideration.

None of the content of this white paper represents legal advice. Legal advice on compliance with the New York SHIELD Act, the GDPR or any other law should be sought from competent legal counsel.

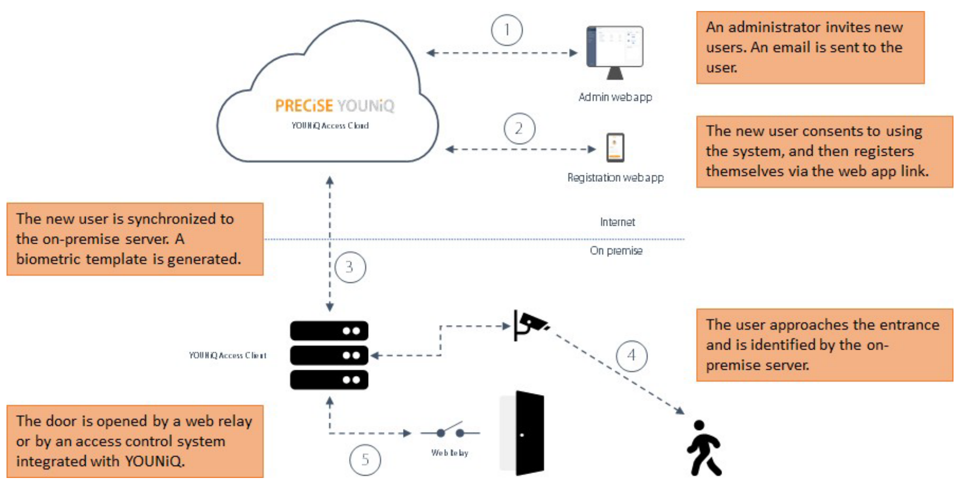
II. How YOUNiQ Works

What most distinguishes YOUNiQ from Internet-scraping biometric technologies is its requirement for consent from the individuals for creating a biometric template from their selfie photo, and using it with the individuals' explicit consent to provide them secure and convenient access to their facilities using YOUNiQ.

The Precise Biometrics YOUNiQ process for security access authentication is simple from the point of view of an individual user that registers for access by submitting a selfie:

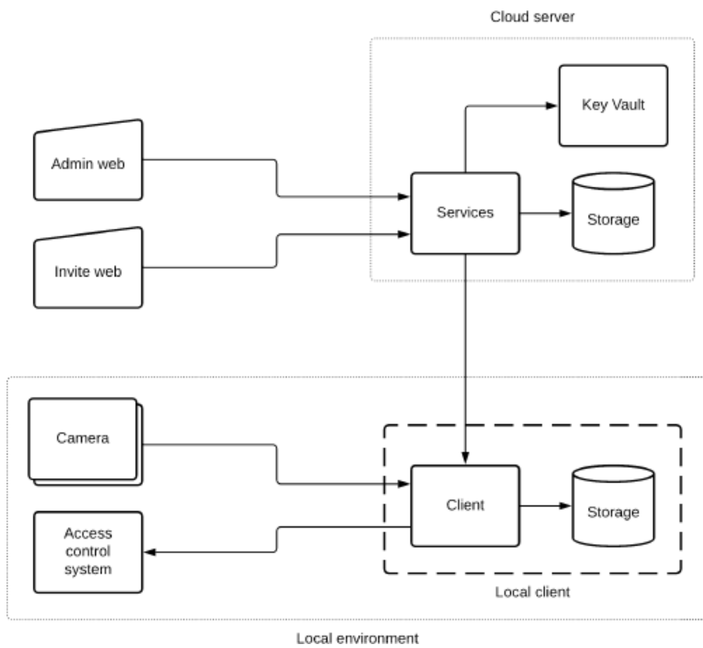


Here is a more technical look behind how the systems operates:



A. How YOUNiQ Creates and Manages Biometric Templates

YOUNiQ creates the Biometric Template from the user selfie on the local client server. It does this by transferring the selfie from the customer's cloud account and creating the Biometric Template in under one second, at which time the selfie is erased from the client server's memory. The selfie is never stored on the client server.



The client server is also where YOUNiQ processes the access authentication from a dedicated local client server on the customers' premises. When an individual approaches a security camera, a facial image is captured and sent to the YOUNiQ local server, where it is converted into a Biometric Template. That template is compared with the authorized users' templates. If a match is found with an authorized Biometric Template, YOUNiQ communicates the match to the customer's security management access system, which grants access to the user, and it is recorded by the Activity Log available to the customer through the secure portal. If no match is found, no such communication is sent. The captured images of individuals seeking access are instantaneously deleted from the local server, as are the Biometric Templates created from them; none of that personal data is retained by YOUNiQ.

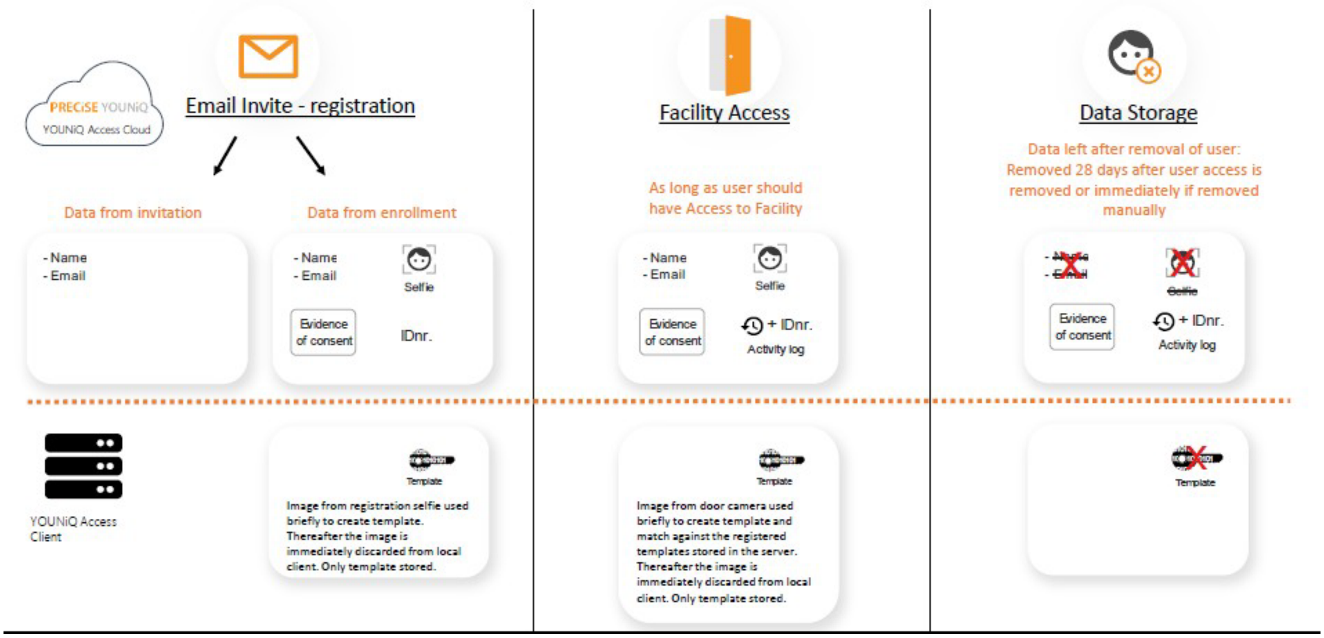
A user can be removed from the system through the secure client portal, which results in the deletion of the user's selfie from the cloud server, and deletion of the user's Biometric Template from the customer's YOUNiQ client server.

III. How YOUNiQ Segregates User Data

User data segregated between Cloud Portal and Local Client Server, separates the Biometric Template away from any other user personal information and selfie image. Additional privacy-by-design components provide an array of supplementary data protection measures.

A. YOUNiQ's Data Minimization and Segregation By Design

YOUNiQ's data flows reflect its privacy-by-design approach, minimizing data storage and securely storing user information in separate repositories, as shown below:



YOUNiQ's privacy-by-design wisely separates the Biometric Template from other user information. Thus, there are two YOUNiQ data repositories for each customer:

1. YOUNiQ's Secure US-based Cloud Portal
2. The Customer's Dedicated Local Client Server

A transparent discussion of the storage of user data on these two repositories follows.

B. YOUNiQ's Secure US-Based Cloud Portal for Customers

One is the secure portal, hosted at a U.S.-based Microsoft Azure cloud server, through which a customer can access the organization's YOUNiQ user data stored in an encrypted repository. These are the customer's data encrypted and secured within YOUNiQ's Azure cloud:

(1) Activity Log: Records of all instances when users are granted biometric-authenticated access to the customer's facility;
(2) User name and e-mail: Record of user's name and e-mail address;
(3) Evidence of Consent: Documentation that a particular user consented to YOUNiQ's use of their selfie photo for biometric access purposes;
(4) Each user's selfie photo: When a new user registers and submits a selfie, that selfie is stored within YOUNiQ's secure cloud portal so it may be available to create the proprietary

biometric template that is critical to the facial recognition functionality. The selfie is stored for generation of updated Biometric Templates as the technology evolves.

Selfies Are Double Encrypted. Not only are these selfies stored in an encrypted and access-controlled cloud environment, each is separately encrypted using 256-bit encryption keys. These encryption keys are unique to each customer organization, and further strengthens the separation of organization's data in the cloud. The encryption keys are stored securely using Microsoft Azure's Key Vault, which is hardware supported for increased security and enforces strict access controls.

The selfie image is retained for future access in the event that YOUNiQ's technology evolves and enables more sophisticated biometric templates, so that an updated biometric template can be generated without requiring a new selfie be taken; and

(5) YOUNiQ ID Number: randomly generated, not associated with a password.

The YOUNiQ Access cloud server stores data in a US-based Microsoft Azure database platform network. Within the Azure network, organizations' data are separated via strict access and security controls, ensuring that different Azure customers cannot gain access to each other's networks and information. Data is protected (both at rest and in transit), utilizing an access-controlled database that is encrypted and regularly backed up. These databases are physically segregated, thereby providing redundancy and increased security.

Within the YOUNiQ Access application, all customer personal data is stored encrypted and kept separate from associated selfies in the cloud server. Information belonging to different organizations within YOUNiQ Access is also kept logically separate, with access to any information requiring specific access rights and being a member of the owning organization.

Stored selfies are encrypted using a separate encryption key per selfie, and using state-of-the-art encryption algorithms. This selfie encryption key in turn is encrypted using a unique encryption key for each organization, also referred to as "key wrapping." The selfie key is then stored in an unreadable format adjacent to the selfie, and the organization encryption key is stored in an Azure Key Vault. Access to a key vault requires proper authentication and authorization before an application is given access, and then only to the application's own keys.

In summary, the YOUNiQ Access cloud server utilizes strong security controls available from the Microsoft Azure platform network to safeguard the processing of sensitive data.

C. The Second User Data Repository: Dedicated YOUNiQ Local Client Server on Customer's Premises

YOUNiQ's privacy-by-design approach calls for separation of the Biometric Template from the user's other personal information, including the user selfie. The second data repository is a dedicated YOUNiQ server installed on the customer's premises. This local client server holds the software that operates YOUNiQ and stores just two types of data items; biometric templates and cloud access tokens.

1. YOUNiQ's Biometric Template

Users' selfies are sent from Precise Biometrics' cloud server to customers' local client servers via encrypted tunnels. The customers' local client server, provided by Precise Biometrics, stores and compares biometric templates with those associated with users approaching the camera-monitored entrance. Communication between the cloud server and the local client is protected with industry- standard transport encryption, using Transport Layer Security ("TLS"), version 1.2, with 2048-bit RSA keys. The local client server uses a unique access token to access the privileged Application Programming Interface ("API") exposed by the cloud server. The token is set up during installation by the technician and can be revoked at any time. If it is revoked, then the local client loses the ability to send and receive data from Precise Biometrics' cloud server.

Once the selfie hits the customer local client server, YOUNiQ's technology uses it to create a proprietary biometric template to be used by the system for authentication. The selfie image is then promptly deleted from the local client server – only a double-encrypted copy remains, and is segregated on the YOUNiQ cloud portal.

What remains on the customers' local client server -- after the selfie is deleted -- is the biometric template created from the selfie, which is used by YOUNiQ to accomplish biometric authentication when the user appears in video. That biometric template is stored using strict access control on the local client server until needed for authentication. The template is proprietary, meaning it can only be usable with the algorithm provided by Precise Biometrics, contains no other personal information about the user, and it cannot be reversed. The Biometric Template reveals no interpretable personal biometric information about a user. It is designed to prevent reverse engineering, and thus cannot reveal users' personal biometric details if examined or acquired by hackers.

2. YOUNiQ's Cloud Access Token

A token generated by the cloud-based YOUNiQ application and installed manually onto the local YOUNiQ client server to permit communication among both servers, and transfer of the customer's data for authentication and activity logging purposes. The cloud access token contains no personal information, and has no relation to anything, except that it exists both at the local client and in the cloud server.

To revoke a local client's access to the cloud the Cloud Access Token is deleted on the cloud side, thus preventing future access.

IV. Compliance with America's Foremost Biometric Privacy Law: Illinois' Biometric Information Privacy Act

In 2008, Illinois enacted the Biometric Information Privacy Act ("BIPA") [1] requiring companies to obtain consent from individuals before collecting or storing biometric information such as fingerprints, retina or

[1] Illinois Biometric Information Privacy Act, 740 ILCS 14/1 et seq. ("BIPA").

iris scans, voiceprints, and hand and face geometry. BIPA authorizes courts to award monetary damages to any person "aggrieved" by a violation of the Act.[2]

BIPA prohibits the collection or retention of biometric information without first:

(i) Informing the subject that the information is being collected;
(ii) Informing the subject of the specific purpose of the collection and the length of time the information is to be stored/used; and
(iii) Receiving a written release executed by the subject or their legally authorized representative.

BIPA also requires covered entities, under certain circumstances, to "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. . . . [and] comply with its established retention schedule and destruction guidelines." Further, a company in possession of biometric information must store, transmit, and protect from disclosure all biometric identifiers and information "using the reasonable standard of care within the private entity's industry," and in a manner "that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."

These requirements are challenging, if not impossible, for biometric technology that scrape facial images from the Internet, given their lack of connection with the subjects from Illinois. In contrast, YOUNiQ's approach provides a platform that embraces, in fact requires, subject consent, and enables organizations to meet the full range of BIPA compliance. Companies should consult with counsel and implement standardized processes and policies to satisfy these and the other requirements of the Act.

V. Compliance with America's Broadest Cybersecurity Law: The New York SHIELD Act

This white paper looks to the New York SHIELD Act[3] as the foremost United States state law imposing reasonable cybersecurity safeguards, which went into effect in March 2020. Most U.S. states have data breach notification laws such as the SHIELD Act, which sometimes impose obligations and fines. The SHIELD Act adds a new dimension of data protection: substantive cybersecurity requirements.

The SHIELD Act is a "possession statute", asserting global jurisdiction of any organization possessing any New Yorker's "private information." And comes with $5,000 fines per violation.

---

[2] In 2019, the Illinois Supreme Court ruled that individuals need not suffer actual harm in order to sustain claims under BIPA. Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Jan. 25, 2019). See "Collecting Biometric Information Just Became Riskier Under Illinois Law," Patrick J. Burke and Alisha L. McCarthy, Pratt's Privacy & Cybersecurity Law Report, April 2019, Vol. 5 No. 3, https://www.phillipsnizer.com/siteFiles/27112/Article-Collecting%20Biometric%20Info%20Just%20Became%20Riskier%20Under%20Illinois%20Law%20-%20Pratts_Privacy_Cybersecurity_April%202019.pdf.

[3] The New York "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act), N.Y. Gen Bus. Law§ 899-bb.

Organizations complying with the New York SHIELD Act are meeting the highest standards for general business organizations, although there are many other legally-obligated U.S. cybersecurity standards within particular critical industry sectors, government contractors and other sectors such as healthcare. The SHIELD Act deems that organizations regulated by government agencies are deemed "compliant" with the SHIELD Act, specifically including entities regulated by:

- Title V of the federal Gramm-Leach-Bliley Act
- The Health Insurance Portability and Accountability Act
- The Health Information Technology for Economic and Clinical Health Act
- NYS Department of Financial Services Cybersecurity Regulation
- "[A]ny other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

If you are a small business, the SHIELD Act has a vaguely defined customized requirements for smaller organizations. They will be deemed in compliance if they implement safeguards that are "reasonable" and "appropriate" for the size and complexity of any organization with:

- Fewer than 50 employees
- Less than $3 million in revenues in each of last 3 fiscal years, <u>OR</u>
- Less than $5 million in year-end total assets per GAAP

Note that the SHIELD Act's requirements still fall upon these smaller organizations.

The Act authorizes the New York State Attorney General to bring legal actions to enjoin violations of the SHIELD Act and obtain civil penalties, up to $5,000 per violation of the cybersecurity safeguards. It grants no private right of action, but plaintiffs surely will cite violations of the SHIELD Act – whether alleged or charged by New York State's Attorney General – as a standard of care. As other states enact laws mandating cybersecurity safeguards for their citizens' personal data, the SHIELD Act safeguards likely will serve as a model and standard in private cases brought by those injured directly or indirectly by failures to maintain mandated cybersecurity safeguards.

Given the potential nationwide sway of the SHIELD Act, it makes sense to consider how YOUNiQ customers can assure compliance with the Act's mandatory "reasonable safeguards." And how Precise Biometrics imposes those safeguards on all data related to YOUNiQ's operation.

A. Does the User Data on the YOUNiQ Secure Portal Fit the Definition of "Private Information" in the SHIELD Act?

The SHIELD Act defines "private information" the same for data breach notification and cybersecurity safeguards. "Private information" is partially a sub-set of "personal information, which is defined as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." Thus, the user data on the secure portal – name, e-mail address and selfie image – all likely fall within New York's definition of "personal information."

However, the SHIELD Act's definition for "private information" – the types of information that triggers the Act's obligations for data breach notification and cybersecurity safeguards – involves a combination of personal information with a checklist of "data elements":

> "1. *Personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:*
>
> - *social security number;*
> - *driver's license number or non-driver identification card number;*
> - *account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;*
> - *account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or*
> - *biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity;* ***OR***
>
> 2. *a username or e-mail address in combination with a password or security question and answer that would permit access to an online account."*

This suggests that the personal information stored on the YOUNiQ secure portal may not even qualify as "private information" because it is not combined with any of the "data elements" enumerated in the definition. The Biometric Template would qualify as "biometric information", but it is not stored in the YOUNiQ secure portal. Rather, the biometric template is stored separately on the customer's local client server.

Similarly, the encrypted data on the YOUNiQ secure portal might appear not to quite fit the definition of "private information" which requires "*the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired."* The key for the encrypted selfie is stored in an unreadable and encrypted format next to the selfie, and the "wrapping" key protecting the selfie key is stored securely in an Azure Key Vault. If so exempted – and this white paper does not consist of legal advice on that or any other legal issue raised herein -- then even a successful hack of the encrypted selfie photo on the secure portal would not qualify as a reportable breach under the SHIELD Act.

Precise Biometrics strongly urges its customers to take SHIELD Act compliance seriously with respect all personal data related to its YOUNiQ installation, do not assume that it ensures SHIELD Act compliance.

We at Precise Biometrics carry on our European tradition of personal data protection and make considerable efforts and expense toward our own compliance with the SHIELD Act.

To facilitate customers' compliance with the SHIELD Act, the remainder of this white paper will focus attention on aspects of YOUNiQ technology that relate to the Act's mandatory reasonable safeguards.

B. The SHIELD Act's Mandatory Reasonable Safeguards

Let's look at the administrative, technical and physical safeguards that the SHIELD Act requires be implemented by any organizations in the world holding New Yorkers' private information, and consider how they might apply to the small footprint of encrypted data used in the operation of YOUNiQ. Note that these safeguards apply to both Precise Biometrics' internal operations and those of YOUNiQ's customers in its operation of the technology.

1. Reasonable Administrative Safeguards

a. Designates one or more employees to coordinate the security program

Must be an employee or the organization (not outsourced to a non-employee).

a. ***Precise Biometrics*** has appointed a US Chief Information Security Officer reporting directly to Precise Biometrics' corporate leadership, responsible for implementing and ensuring compliance with the Precise Biometrics' policies and procedures designed to ensure compliance with the NY SHIELD Act, Illinois' BIPA, GDPR and other applicable laws.

b. ***Customers*** should designate a coordinator for their security program if they have not already done so. The employee coordinates the policies and procedures that make up the security program as they apply to the YOUNiQ server and any dataflows with camera, security access or other applications on the customer's network, and ensure legal compliance.

b. Identifies reasonably foreseeable internal and external risks

Risk assessments – performed to identify reasonably foreseeable internal and external risks -- are key to a security program. Those assessments usually are updated at least annually, sometimes the process outsourced for independence.

a. ***Precise Biometrics*** – It is the responsibility of the US Chief Information Security Officer, in conjunction with the IT manager, to regularly review the company's operations and assess risks as they pertain to the security of company information, private information and data elements. These reviews rely on guidance from NIST, ISO or other regulatory or certification agencies, and when appropriate, independent third-party consultants. Beyond review of local IT infrastructure and associated practices/procedures, these assessments also include review of externally supplied IT services, such as Microsoft Azure. Given some of these cloud services are used in the deployment of the Precise

Biometrics YOUNiQ product, which involves the storage of private user information (e.g., selfie images), regular review of how these providers address cybersecurity safeguards is important.

b. ***Customers*** should make sure their security coordinator includes the YOUNiQ installation in its risk assessment and ensure appropriate use of encryption and strictly limiting permissioned access to related personal information.

c. Assesses the sufficiency of safeguards in place to control the identified risks

The SHIELD Act requires administrative compliance with the risk assessment process, including a commitment to act on remediating gaps identified in Risk Assessments, implementing controls and identifying any residual risk even after the controls were applied.

a. ***Precise Biometrics*** – Should risk assessments identify previously unknown threats or vulnerabilities, the company will make reasonable efforts to eliminate them or implement safeguards to control such potential threats or vulnerabilities. Moreover, if it is determined these vulnerabilities resulted in a breach of information security, any customers or partners of the company will be notified in a timely manner of the breach, along with actions to be taken by the company to correct the safeguard deficiency leading to the breach.

b. ***Customers*** should be sure that the storage of their YOUNiQ data, and any camera or security access processes to which it is connected, are the subject of the risk assessment, and that any controls identified to mitigate any discovered risks are implemented, tested and re-evaluated each year.

d. Trains and manages employees in the security program practices and procedures

Once you have policies and procedures, these need to be learned and understood by the employees intended to carry them out. For employees, there are many important best practices to learn, including how to avoid phishing attacks on the organization's systems.

a. ***Precise Biometrics*** conducts and documents regular employee training on data security, including specifically for processing, storage and deletion of YOUNiQ users' data.

b. ***Customers*** should insure that employees responsible for handling of YOUNiQ systems are trained in security protocols for protection of that data, including proper maintenance and upgrading of their YOUNiQ systems. It is important to document all training, to demonstrate to regulators that it in fact took place and the content of the training.

e. Selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract

The SHIELD Act makes organizations responsible for appropriate vendor management, particularly into any service providers holding New Yorkers' personal information. Organizations must require by contract that service providers also use appropriate safeguards.

Precise Biometrics – Our vendor selection process includes assessment of their privacy and data security safeguards, and contractual commitments as to the same. The above mentioned risk assessment reviews are included as part of the company's vendor selection and management process, and to the extent possible the company's vendors are required to implement comparable information and cybersecurity safeguards.

Customers should closely examine YOUNiQ's data protection safeguards, and those of all other service providers used for its access security systems, including camera, access control and entry systems.

f. Adjusts the security program in light of business changes or new circumstances

Risk assessment must be triggered when a significant new data-handling system is implemented on an enterprise's network, to determine whether there might be risks requiring controls. Recognition of such increased risk may result in changes or adjustments to the organization's security program.

Precise Biometrics follows EU GDPR's privacy-by-design approach to changes made to YOUNiQ, reducing data protection risks in advance as built-in compliance of all data processing and storage. New versions of YOUNiQ are tested, including penetration testing, before release for customer use. Precise Biometric's Chief Information Security Officer and YOUNiQ product management meet regularly to consider updated risk assessments and inquire as to new external and internal threats, including changes in the cybersecurity threat vectors, including the latest hacking techniques, and include updating of our incident response plan. These assessments are also undertaken in the event the company becomes aware of substantive changes to relevant federal or state regulations.

Customer should consider the implementation of YOUNiQ a new circumstance triggering a risk assessment and consideration of any required controls to mitigate risks, including a review confirming all YOUNiQ-related data is appropriately encrypted and permissioned access is extremely limited.

2. Reasonable Technical Safeguards

a. Assesses risks in network and software design

The SHIELD Act requires that risk assessments include analysis of risks in network and software design. Effective network design includes proper asset inventories and segmentation when appropriate. The integrity of the network should be tested with penetration testing and vulnerability analyses.

Precise Biometrics **–** YOUNiQ's privacy-by-design approach attends closely to inclusion of data protection features and control of risks. To identify network vulnerabilities Precise Biometrics engages an independent third-party on an annual basis to have conducted a network penetration test, the results of which guide the company's decisions regarding network usage policies and investment in infrastructure and services.

Customer - Precise Biometrics YOUNiQ customers are encouraged to include its YOUNiQ and related security systems in its risk assessments, and conduct penetration tests and/or vulnerability scans that include those systems.

b. Assesses risks in information processing, transmission and storage

Information processing, transmission and storage must be studied for risk, part of the risk assessment and overall security plan. These risks include hackers and insider threats. Each enterprise faces its own array of risks to control, depending on the maturity of the cybersecurity program.

Precise Biometrics employs its Information and Cybersecurity Policy to provide its employees guidance on the proper and safe management of information. This policy includes specific guidelines and safeguards associated with information processing, transmission and storage. These processes are regularly assessed for potential new risks, and new controls are then put in place.

Customer We encourage YOUNiQ customers to regularly assess risk related to the processing, transmission and storage of data used by YOUNiQ and related security systems. With those risks identified, the company is better enabled to develop customized Information and Cybersecurity Policy to provide their employees specific guidelines and safeguards associated with processing, transmission and storage of security systems' personal information, and its timely deletion from all systems.

c. Encryption in transit and at-rest

The organization must assess whether it is appropriate to encrypt data in transit and at-rest, and what form of encryption in each instance.

Precise Biometrics' YOUNiQ Access utilizes state-of-the-art encryption algorithms during storage and transmission of all customer personal data, including selfies. Additionally, Precise Biometrics' Information and Cybersecurity Policy requires that all hard drives and servers be encrypted using available OS (i.e., Windows10) security tools such as BitLocker. Internal (LAN) file transmission is also encrypted, again using available OS security tools. External file transmissions are executed in a secure manner, generally involving cloud services (e.g., Dropbox) which utilize encryption (e.g., HTTPS), and are password protected. Passwords are sent to receiving parties via separate communication.

Customer Precise Biometrics YOUNiQ customers are encouraged to implement appropriate data encryption within their organization.

d. Detects, prevents and responds to attacks or system failures

Detecting attacks and system failures requires monitoring, creation and storage of activity logs, and regular analysis of those logs for evidence of attempted intrusions. Preventing attacks and system failures involves vigilance of new threats. Important is having an incident response plan and team, with regular practice and tabletop exercises. Finally, having written business continuity and disaster recover planning, for post-attack resilience.

Precise Biometrics' YOUNiQ Access records and logs all instances when users are granted biometric-authenticated access to a customer's facility. These logs are accessible by customers through the YOUNiQ secure cloud portal. Within the organization, Precise Biometrics implements virus protection among all PCs, laptops and servers within its organization, and subscribes to an independent network monitoring service. Detected attacks are logged and analyzed for inclusion in periodic risk assessments. Moreover, detects that result in a breach of information security, any customers or partners of Precise Biometrics are notified in a timely manner of the breach, along with actions to be taken by Precise Biometrics to correct the safeguard deficiency leading to the breach.

Customer **–** Precise Biometrics YOUNiQ customers are encouraged to implement appropriate antivirus and network monitoring solutions. Customers are also encouraged to regularly review logs of biometric-authenticated access to their facility.

e. Regularly tests and monitors the effectiveness of key systems

Organizations' security program must assure the effectiveness of key systems. Monitoring tends to be performed by in-house IT security staff, while testing by independent consultants has credibility advantages. Processes and procedures are used to document the testing and monitoring program.

Precise Biometrics - As previously mentioned, and as part of its regular risk assessment policy, Precise Biometrics utilizes external penetration testing and monitoring services to identify vulnerabilities, including using independent consultants.

Customer **–** Precise Biometrics YOUNiQ customers are encouraged to implement appropriate vulnerability testing of their IT/network infrastructure.

3. Reasonable Physical Safeguards

a. Assesses risks of information storage and disposal

Security procedures for physical access to computers and servers, procedures for disposal of media containing data, miscellaneous physical safeguards such as clean desk policies.

Precise Biometrics Physical access to the location of Precise Biometrics' US operation is protected by a card access system, with further access to Precise Biometrics' office space protected by card and biometric (YOUNiQ Access) authentication. Precise Biometrics' US IT infrastructure is additionally protected, being located in a key accessible data closet.

Customer The local YOUNiQ client server should receive physical protection methods, such as installation in a locked space with limited access. It is also possible to encrypt the hard drive as an additional security measure; this would be handled by the operation system and protected by the system user's password.

b. Detects, prevents and responds to intrusions

This includes systems to detect and prevent physical intrusions on premises, particularly with respect to information systems, including strong locks, video monitoring, and appropriate use of encryption. Response procedures include robust protection for the information systems in backup environments.

Precise Biometrics – Building entrances are continuously monitored for propped door openings, with security personnel dispatched as necessary. Video monitoring is also deployed throughout the location of Precise Biometrics' US operation.

Customer - To the extent reasonable, Precise Biometrics YOUNiQ customers are encouraged to implement appropriate monitoring of their facilities.

c. Protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information

These protections include thorough oversight of access permissions on a least privileged basis, encryption of data in transit and at-rest, access authentication (multi-factor and risk-based), and protections on remote computing, including use of secure Virtual Private Networks and mobile device safeguards. Published policies for employees and third-party service providers, including approval and dissemination of an acceptable use policy, vendor management policy and appropriate training for employees.

Precise Biometrics' Information and Cybersecurity Policy regulates the logical and physical access to information and data, by both employees and when appropriate, third parties. Logical access tools include diligent password policy and practices. Employees working remotely access Precise Biometrics' resources and information (Precise Biometrics domain) via password protected virtual private network (VPN) connectivity.

Customer - To the extent reasonable, Precise Biometrics YOUNiQ customers are encouraged to implement appropriate logical and physical access safeguards. For example, limiting physical access to the YOUNiQ local client server and wherever related security system data is stored and transported.

d. Disposes of private information with a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed

Logging of data and scheduling destruction based on business purpose. Policy and procedures for data destruction.

> ***Precise Biometrics*** – YOUNiQ user data that is no longer required for active use or archival purposes is regularly and permanently deleted. This includes requests by owners of personal information (e.g., selfies provided during YOUNiQ user registration). Information in physical form is shredded prior to disposal.

> ***Customer*** - To the extent reasonable, Precise Biometrics YOUNiQ customers are encouraged to implement appropriate procedures for deleting and disposing logical and physical information, respectively. If you are subject to the Illinois BIPA, keep in mind its requirement to develop a written policy, made available to the public, establishing a retention schedule and guidelines for destroying biometric identifiers and biometric information.

e. Prepare and preserve documentation of compliance activities

Documentation confirms the seriousness of an organization's risk-based policies, procedures, and specific measures taken by the organization in response to assessed risks, and their outcomes. It also provides important evidence to support the organization's adherence to its own policies and procedures, and compliance with the SHIELD Act, allowing state investigators to review risk assessments, evidence of controls put in place and identified remaining risks, and testing results. As employee training is a key component on compliance, the organization should retain documentation of its employee training programs and attendance by employees. Similar documentation should be maintained with respect to third party service providers.

> ***Precise Biometrics*** documents via internal memo all activities associated with maintaining SHIELD Act compliance, including but not limited to meeting minutes, risk assessment reports, penetration test reports, and logs of any known attacks against Precise Biometrics' IT/network infrastructure.

> ***Customer*** - To the extent reasonable, Precise Biometrics YOUNiQ customers are encouraged to implement appropriate recordkeeping of relevant information and cybersecurity activities they employ.

VI. Conclusions

US businesses seek biometric security solutions that transparently comply with US law, including the cybersecurity safeguards required by New York's SHIELD Act, which has nationwide reach, and the biometric consent requirements of Illinois' BIPA law which applies to Illinoisans. The GDPR principles that guided the design of YOUNiQ in Sweden provide an excellent foundation for US data privacy and cybersecurity compliance. This includes:

- **Reasonable Cybersecurity Safeguards**: This white paper offers a discussion of issues relevant to transparent compliance with the New York SHIELD Act, in particular its requirements for reasonable cybersecurity safeguards. YOUNiQ is dedicated to SHIELD Act compliance, rightly of first importance to US businesses comparing alternative biometric security technology.

- **Data Minimization, Segregation and Encryption**: YOUNiQ works with minimal personal data from users, segregates it both physically and logically, and double-encrypts the user's selfie. The proprietary YOUNiQ biometric template cannot be reverse engineered. This segregation, encryption and engineering enhances SHIELD Act compliance. The SHIELD Act's definition of "personal information" may not even apply when – as with YOUNiQ – a selfie photo is effectively encrypted and the encryption key is stored elsewhere and not susceptible to being obtained by a hacker.

- **Consent, Purpose and Storage Limitations**: YOUNiQ provides users with an opportunity to consent or decline to have their personal data collected, and to have it deleted when requested or no longer necessary for biometric purposes. YOUNiQ's privacy-by-design approach to consent supports compliance under GDPR, the SHIELD Act and Illinois' BIPA.

US data privacy and security laws and regulations are moving in the direction of the stringent data protection regulatory framework already in place in Europe. YOUNiQ offers US businesses a technology designed from start-to-finish for GDPR – and now US – compliance.