BioID®
be recognized

BioID Whitepaper on GDPR Ready Biometrics

July 2019

1 Introduction

In the year 2018, the two buzzwords for companies operating online have certainly been GDPR and KYC. Although very different at first glance, interestingly, the General Data Protection Regulation (GDPR) does have similar impact on the significance and use of biometrics as the Know Your Customer (KYC) regulatory. Both oblige companies to authenticate their customers with high levels of assurance (LoA).

To reduce fraud and ensure business, banks, companies, governments and individuals need to be able to tie a physical person to their digital identity. In order to comply with GDPR, they have to be able to prove explicitly that the given consent, the changes made to data or the authorization of actions have certainly been issued by the respective individual. When also taking frictionless user experience and process automation into account, biometric authentication is the most intuitive way to do so.

But can highly sensitive biometric data really be used to secure identities and their data in a GDPR compliant way?

Yes.

2 GDPR compliant system architecture

BioID is based on "privacy by design" as well as "privacy by default" principles, allowing online service providers, and the financial industry in particular, to benefit from BioID's GDPR readiness. The privacy-assured technology supports the implementation of KYC relevant strong customer authentication (SCA). To fulfill this target, BioID's service has been built with a special "secure by design" architecture:

- We reduce raw data to pseudonymized binary templates in order to avoid superfluous information. In privacy-mode, raw data is deleted by default right after use and only kept for support if requested by the customer.
- Active participation in any BioID authentication application is guaranteed through liveness detection: With randomized directional movement and sophisticated texture analysis BioID implements industry-leading fraud prevention. Unintended authentication as well as spoofing through photo and video replay attacks is eliminated.
- Pseudonymized binary templates are stored without other personally identifiable information (PII) in a highly secured cloud with European data centers. Due to a proprietary format, the template is unusable outside of BWS. In addition, it is irreversible and revocable.
- Multiple security mechanisms have been implemented against unauthorized access of biometric data: Transport encryption, comprehensive liveness detection and especially high recognition accuracy of 99.9%.
- Full transparency concerning processing of data, data handling and storage is provided: Any customer has full access to their data and can view, modify and delete their data and accounts. Processes can be reviewed in the BioID Terms of Service and Privacy Policy.

Your biometric data belongs to you and only you!
We can recognize you, but we don't know
who you are.

3 Detailed Compliance Assessment

3.1.1 Principle lawfulness, fairness and transparency (Article 5(1)(a) and (b), 6-10 as well as 12-14 GDPR):

- Data processing solely for the purpose of providing biometric recognition within the BioID Web Service (BWS)
- Users are fully informed about data collection and processing and stay in full control of their information
- We insist on GDPR compliance of our partners

3.1.2 Principle purpose limitation (Article 5 (1)(b) GDPR):

- Collection and usage only of those data that are directly needed for the process of biometric authentication
- Usage of data solely for the purpose of providing biometric operations within the BioID Web Service (BWS)

3.1.3 Principle data minimization (Article 5 (1)(c) and (e) GDPR):

- Only data needed for biometric operations are processed: No other personally identifiable data is requested, e.g. names or addresses.
- Raw data is obliterated immediately after processing
- Certain BioID services (e.g. PhotoVerify, Liveness Detection) explicitly designed to not store data at all.

3.1.4 Principle accuracy (Article 5(1)(d) GDPR):

- BioID Auto-Enrollment for automatic updating of biometric data
- Empowered customers have full control over data and can modify as well as delete
- Automatic deletion of accounts and data after certain time of inactivity

3.1.5 Principle storage limitation (Article 5(1)(e) GDPR):

- Raw data transformed to pseudonymized binary templates
- Superfluous information avoided
- Raw data discarded by default right after use and only kept for support if requested by the customer

3.1.6 Principle integrity and confidentiality (Article 5(1)(f) and 32 GDPR):

- Multiple security mechanisms against unauthorized access see BioID TOMs
- Strict separation of biometric data and other personally identifiable data
- Irreversible, revocable template
- Transport encryption
- Highly secure cloud provider with European data centers
- Comprehensive liveness detection, highly secure face recognition

3.1.7 Principle privacy by design (Article 25 GDPR):

- Privacy-assured pseudonymized service
- Automatic deletion of data not needed in the future
- No data collected other than needed for the purpose of providing the BioID Web Service (BWS)
- Built-in "right to be forgotten" with self-sovereignty of the customers

4 BioID – Ready for GDPR & KYC

About BioID

BioID is the cloud biometrics company with advanced liveness detection. Our face recognition service is provided with a special focus on data privacy, reliability and security. Guided by the vision that anonymous biometric authentication empowers internet users to secure their online identities with privacy, BioID offers a reliable link between a real person and their digital identity. This is performed by verifying the user's presence in a convenient and natural way – just the way you look. BioID's patented liveness detection and the PhotoVerify technology make automated online "face-to-face" identity proofing possible.

Privately held with R&D based in Germany, BioID has offices in Switzerland and the US and its technology has been proven through many years of use at enterprises, banks and government organizations.

Liveness detection

To guard against attackers using photos or recordings of a user, liveness detection ensures that the sample is captured from a live user. For GDPR readiness, this is the key to gain effective "user consent" and secure accounts against misuse. BioID's patented system uses motion analysis to detect the difference in movement between a 2D photo and a 3D face. By directing the user to move in a certain way and then verifying that the instructions are followed, video attacks can also be blocked. In addition, the powerful "Replay Defender" detects displays through texture analysis and prevents unauthorized access through videos and even animated 3D avatars!

Anonymity

In order to protect user privacy, BioID keeps biometric data anonymous with no usernames or other personally identifying information. BioID stores no raw images, only a biometric template: a mathematical representation of the user's unique features, from which an image cannot be reverse engineered. So even if biometric data were compromised, it would be virtually useless to an attacker, and the service provider could simply delete any such templates and allow the user to re-enroll under a new anonymous ID.

BioID. Forget Passwords. Be Recognized.