BioID
be recognized

GDPR Compliance with BioID Web Service

1

GDPR Compliance & the Rise of Biometric Services

Following the implementation of the European Union's **General Data Protection Regulation** (GDPR) since May 25, 2018, the world has experienced a shift in data privacy paradigms. As industries faced the consequences of this regulation, another trend gained momentum: the expanding use of biometric data, particularly facial recognition, for identification and verification.

The GDPR's impact and rules have created a framework for personal data protection, defining biometric data as personal, and sensitive hence requiring specific consent for processing. In this context, 2018 saw the implementation of not only GDPR but also an increase in Know Your Customer (KYC) rules and/or guidelines, both of which reinforced the need for high-assurance client authentication.

Furthermore, new and emerging AI-powered biometric services, which are high-performance and extremely accurate, did rise to the instance, enabling a wide range of secure and privacy-assured online services not possible before.

However, the critical question remains: Can organizations subject to GDPR use these biometrics for their end-users?

The short answer is yes!

This whitepaper provides an overview of BioID's Web Service in light of GDPR.

2

GDPR Compliant System Architecture

BioID stands for the principles of „privacy by design“ and „privacy by default,“ offering solutions to online service providers, as a “data processor” in accordance with GDPR classification. Our privacy-assured technology enables the implementation of strong customer authentication (SCA) for such as KYC and eIDAS service providers, all classified as “data controllers”. To achieve this goal, BioID has developed a secure and meticulous design as follows:

Privacy Shield Architecture:

The communication between the data controllers and BioID (data processor) uses only pseudonymized data without any **personally identifiable information** (“PII”). Not only does this make hijacking attacks to no avail, data subject is completely shielded from BioID, making the data controller the responsible linkage between the data subject and its corresponding pseudonymized information.

“Zero Footprint” and “Data Minimality”:

BioID‘s commitment extends to data “zero footprint” or „data minimality”. Raw data is by default discarded immediately after each biometric unless explicit demand for storage due to customer support or audit purposes is obligator. For enroll/verify operations, biometric data is translated into encrypted, pseudonymized irreversible binary templates prior to any verification or identification operations.

Active Participation ensures User Consent:

The BioID authentication application ensures active user participation, guaranteeing the user’s consent through liveness detection. The technology provides trustworthy fraud protection by combining randomized directional movement and precise texture analysis. Particularly noteworthy is the system‘s ability to prevent unintentional authentications and spoofing attempts caused by photo and video replay attacks.

Uncompromised Data Security:

The storage of pseudonymized binary templates stands as a testament to BioID‘s commitment to data security. These templates, which do not include personally identifiable information (PII), are housed in highly protected data

centers meeting EU GDPR standards. The encrypted proprietary format ensures that the templates can only be used exclusively within the BioID Web Service (BWS).

Security Measures Adhering to Industry Best Practices:

BioID has implemented a multi-layered security infrastructure to safeguard against illegal data access. The biometric data is protected during transmission by transport encryption, and thorough liveness detection algorithms to block any efforts at fraudulent access.

Best-in-class Biometrics with High Performance:

BWS's 99.999% recognition accuracy attests to its leading and continuous commitment to accuracy and security.

BioID's patented system, powered by motion analysis, discerns movement nuances between 2D photos and 3D faces. Precise user movement instructions hinder video attacks, backed by the „Replay Defender" blocking unauthorized access attempts via texture analysis, including animated 3D avatars. No usernames or personal data are stored. Biometric templates are used. In case of compromise, templates can be erased, letting users re-enroll anonymously, upholding security.

Note:

Liveness detection stands as a pivotal defense against attackers leveraging user photos or recordings. Its core role is to ensure data capture exclusively from live users. This not only strengthens GDPR compliance but also establishes robust **user consent**, bolstering account security.

3

BioID's Detailed GDPR Compliance Assessmentssment

Articles	Description	Points of Compliance
5(1)(a), (b), 6-10, 12-14	Principle lawfulness, fairness and transparency	• 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
5 (1)(b)	Principle purpose limitation	• 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)
5 (1)(c) and (e)	Principle data minimization	• 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) have been explicitly designed to not store data at all.

Articles	Description	Points of Compliance
5(1)(d)	Principle accuracy	• 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
5(1)(e)	Principle storage limitation	• 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
5(1)(f) and 32	Principle integrity and confidentiality	• Multiple security mechanisms against unauthorized access • 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
25	Principle privacy by design	• 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

About BioID

As a leader and pioneer in cloud-based biometric services, BioID sets the highest standards for a secure biometric SaaS particularly for online face recognition.

BioID's mission is rooted in the belief that anonymous biometric authentication empowers users to fortify their online identities discreetly. Guided by this vision, BioID seamlessly connects real-world individuals with their digital personas. Via its groundbreaking patented liveness detection and revolutionary PhotoVerify technology, BioID brings self-service unattended "face-to-face" identity validation a reality.

With operations in Switzerland and the USA, BioID is privately held and has its research center in Germany. Years of successful implementation across businesses, banks, and governmental organizations have demonstrated the strength of our technology.

BioID biometrics services can be tested free-of-charge at playground.bioid.com

Be recognized.
Simply by the way you look.