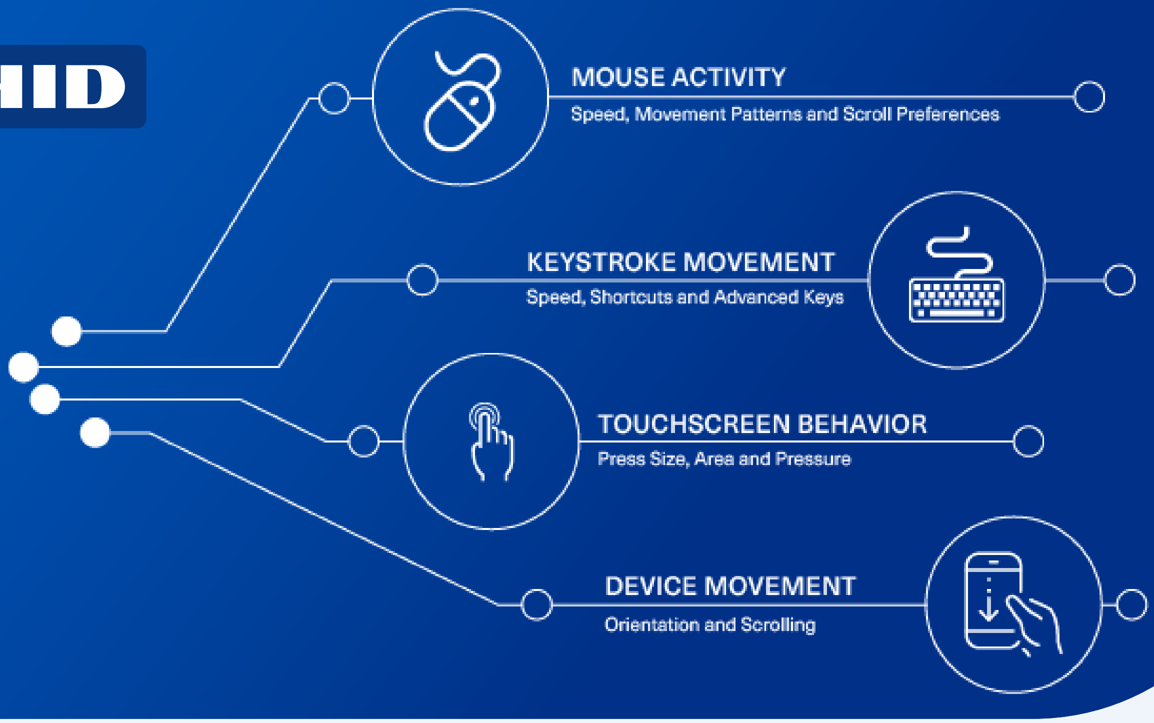


MOUSE ACTIVITY
Speed, Movement Patterns and Scroll Preferences

KEYSTROKE MOVEMENT
Speed, Shortcuts and Advanced Keys

TOUCHSCREEN BEHAVIOR
Press Size, Area and Pressure

DEVICE MOVEMENT
Orientation and Scrolling

Behavioral Biometrics

Privacy & Legal Regulations

Sophisticated digital frauds are rampant throughout the digital world.

Through advanced social engineering methods or by installing various malicious software on users' devices, fraudsters are proving highly creative in coming up with new ways to trick the user into giving up their personal and security details.

Regardless of the method used, the fraudsters' usual goal is to access the victim's bank accounts and steal their money or steal information.

The aim of behavioral biometrics is to achieve a fraud-free digital world by leveraging sophisticated technology to identify unique and measurable patterns in human behavior. Behavioral biometric data consists of actual user activities that characterize the user as a human being. In contrast, there are physical biometrics which include height, weight and of course unique fingerprints and iris scan.

In the context of digital user experiences, behavioral biometrics analyze the user's unique digital behavior to validate the trusted user; and hence stop the abuse of their digital identity.

However, using this technology raises new questions regarding the specific personal data which is collected, processed and protected. Most banks and financial services providers wonder what legislation and regulations are in place to cover the privacy and security aspects of behavioral biometric technology.

This white paper examines the relevance and the legal framework of the EU legislation — mainly GDPR in the area of biometric and behavioral biometric systems and data. More specfically, it explores:

- Privacy standards in Europe and United States
- GDPR definition of Biometric data, processing and consent
- PSD2 Strong Customer Authentication
- How HID Global uses Behavioral Biometrics

WHITE PAPER

What Is Behavioral Biometrics?

Behavioral biometrics is derived from the general premise that one person can be reliably identified by habits, physical features and environments. In the context that is important for this paper, behavioral biometrics is represented by a series of methods for identifying unique and measurable patterns in human behavior. Unlike physical biometrics which include height, weight, and unique fingerprints, iris scan behavioral biometrics is easily transferable to the digital world due to the user's digital interactions and the available data points.

In the physical world, humans have an innate ability to identify and deduce intent of others by observing their behavior. Behavioral biometric technology aims to do just that: to process user behavior data so identity is validated and intent is understood.

Behavioral biometric technology consists of actual user activities (logging in to the application, navigation to a specific page, transaction checkout, etc.) and the data that characterizes the user as a human being (such as mouse movements, typing cadency, touch events, swipe patterns, etc.). Such data sets represent behavioral biometry, which can uniquely characterize a user with a reasonable amount of analysis and proper processing.

Unlike other biometric authentication techniques (fingerprinting, retinal scan, voice recognition, etc.), behavioral biometrics does not need additional devices to create and compare individual profiles.

Approach to Privacy and Biometrics in Europe and the United States

The European GDPR (Regulation (EU) 2016/679 of 27 April 2016 General Data Protection Regulation[2]) is currently considered very stringent and has inspired other data regulations around the world including in the United States. This white paper, therefore, also offers a short summary of behavioral biometrics compliance details for the U.S.

Generally, the regulation of personal data processing in developed countries is progressing swiftly and seems to be slowly evolving in the direction to, in broad terms, correspond with the GDPR or introduce a slightly less stringent standard of care/opt-in requirements.

UNITED STATES OF AMERICA

There is currently no general federation-level regulation of personal data processing similar to GDPR in the US. That being said, the situation may change shortly with the (re-)introduced proposal of the Data Protection Act in 2021 in the US Senate.

Regulation in the US is currently at the state level. Only a handful of US states have a legal regulation covering commercial biometric data use, including California, New York, Texas and Washington.

California's GDPR-inspired CCPA (California Consumer Privacy Act of 2018) is considered to be fairly elaborate. Under CCPA, biometric information processing to uniquely identify a consumer is considered processing sensitive personal information. That is only possible with certain limitations and must be considered within the boundaries of "business purposes," which includes "helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes."

PRIVACY LEGAL FRAMEWORK IN THE EUROPEAN UNION AND THE UNITED KINGDOM

The very first European legislation in the data protection area was the EU Data Protection Directive[3] in 1995, which was created as an essential element of EU privacy and human rights law. This directive was then replaced in 2016 by GDPR. The GDPR is considered the "gold standard" for privacy and data protection regulation which came into effect on 25 May 2018. European Union (EU) Member States had to harmonize their legislation per GDPR Regulation and has served as a model that many other countries around the world are using as a template for their data protection regulations. The adoption of GDPR was a reaction to the constantly growing use of digital services as well as the need to secure personal data.

Since Brexit, the UK has modified GDPR and adopted its own data privacy law that governs the processing of personal data from individuals inside the UK called UK-GDPR. The UK government replaced all mentions of EU institutions with UK domestic institutions and all mentions of other EU legislations was replaced by the Data Protection Act 2018; references to the surveillance authority were replaced with references to the Information Commissioner's Officer (ICO), which is the data protection authority in the UK.

Both GDPR and UK-GDPR bring tools for strengthening fundamental individual rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital market. They build on the three main ideas: transparency, compliance and enforcement.

These pieces of legislation focus on the procedure of collecting and processing personal data from EU and UK residents respectively. GDPR and UK-GDPR rule that the companies need to give people notification ahead of collecting, as well as to obtain explicit consent to collect and store their data. When a data breach occurs, the organization must inform the person about this situation on time.

Without providing such information, the organization is not compliant and therefore subject to a material penalty.

Let us take a closer look at the various legal aspects of behavioral biometrics, including processing rules or the need for explicit consent for dealing with personal data as per GDPR.

GDPR DEFINITION OF BIOMETRIC DATA

The GDPR defines biometric data in Article 4 (14) as:

> *"Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."*

GDPR Article 9 GDPR further states:

> *"Processing of special categories of personal data defines biometric data as biometric data for the purpose of uniquely identifying a natural person."*

According to these articles:

- All biometric data is personal data
- Biometric data allows or confirms the identification of an individual
- Biometric data falls into a special category data when it is processed "for the purpose of uniquely identifying a natural person"
- GDPR recognizes biometric data as subject to sensitive personal data deemed a "sensitive category of personal data"

GDPR BIOMETRIC DATA PROCESSING RULES

As a principle, the processing of special categories of personal data is prohibited according to Article 9 (1) GDPR:

> *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."*

However, collection of biometric data is allowed in specific situations, but only under strict, general processing rules with exemptions only within a restrictive framework outlined in Article 9 (2) GDPR dealing with processing of special categories of personal data including behavioral data.

In case the processing is necessary to:

- Satisfy a contract to which the data subject is a party
- Process the data to comply with a legal obligation
- Process the data to save somebody's life
- Perform a task in the public interest or to carry out some official function
- Fulfil the legitimate substantial public interest to process someone's data

GDPR AND THE NEED OF EXPLICIT CONSENT FOR PROCESSING

Generally, the GDPR requires explicit consent for personal data processing, the more it applies to special categories of personal data. The crucial rule can be found in Article 9, Paragraph 2 (a):

“The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.”

Article 4 (11) of the GDPR defines consent as:

“any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

The explicit consent needs to be also presented to the customer as a choice to decide whether the person agrees with the processing of personal data and under which conditions the organization will process the data.

Moreover, additional conditions apply to consent that must be given expressly, which means in written form or orally, implied consent would be considered not to be sufficient in terms of GDPR.

A person must actively give explicit consent to their biometric data being collected and processed. For example, a bank or other financial service provider must develop a clear and concise way to inform its customers that their biometric data is being collected, how it is stored, how that data is used, and then allow its customers to give or withdraw consent to its collection and processing.

Nevertheless, the ban from using the data does not apply if the processing is necessary for reasons of substantial public interest, based on the union or member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9 (2) (g) GDPR).

The conditions which must be fulfilled altogether to indicate substantial public interest are:

- The processing of the special categories of personal data must be addressed in a specific
- Derogation to Article 9 (1) GDPR in union or member state law
- The provision will have to address the proportionality concerning the pursued aim of the processing and contain suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- The provision under union or member state law will have to respect the essence of the right to data protection
- Processing of the special categories of data must also be seen as necessary for the reason of the substantial public interest, including interests of systemic importance.[4]

Behavioral Biometrics and PSD2 Strong Customer Authentication

The GDPR is intricately linked to other regulations. It must be viewed in conjunction with the second Payments Services Directive (PSD2)[5]. In particular, its Strong Customer Authentication (SCA) Regulatory Technology Standards (RTS)[6] requirement.

PSD2 provides rules for payment security and customer authentication, concentrating on protecting consumer payments made over the internet. For payment security, the directive states that

> *"all payment service providers, including banks, payment institutions or third-party providers (TPPs), will need to prove that they have certain security measures in place ensuring safe and secure payments. The payment service provider will have to carry out an assessment of the operational and security risks at stake and the measures taken on a yearly basis."*

The PSD2 deals with payment security and customer authentication rules and focuses on protecting online consumer payments. It also calls for the need for authentication mechanisms to match the context of the payment transaction with some exemptions such as low-value payments, outgoing payments to trusted beneficiaries, or low-risk transactions based on a transaction risk analysis.

According to the PSD2, payment service providers are obliged to apply SCA when a payer initiates an electronic payment transaction.

The European Commission defines SCA as a process that *"validates the identity of the user of a payment service or of the payment transaction."*

SCA is based on the use of two or more authentication elements:

- **Knowledge –** something only the user knows, e.g., a password or PIN
- **Possession –** something only the user has, e.g., a card, a One-Time-Password (OTP) hardware token or mobile phone
- **Inherence –** something the user is, e.g., via biometric authenticator such as fingerprint,voice, eye-print

Conversely, behavioral biometrics are a great asset because they comply not only with GDPR requirements but are also compatible with SCA as another element based on inherence.

While it is not entirely clear whether or not the PSD2 regulation supersedes the GDPR-based prohibition of processing of special categories of personal data (the references seem to be circular — the GDPR refers to other legislation, such as PSD2, for specification of the public interest and at the same time the PSD2 requires processing in compliance with data processing legislation such as the GDPR).

Such security serves both the customer (protection of their finances) and the public (inhibition of fraud in general).

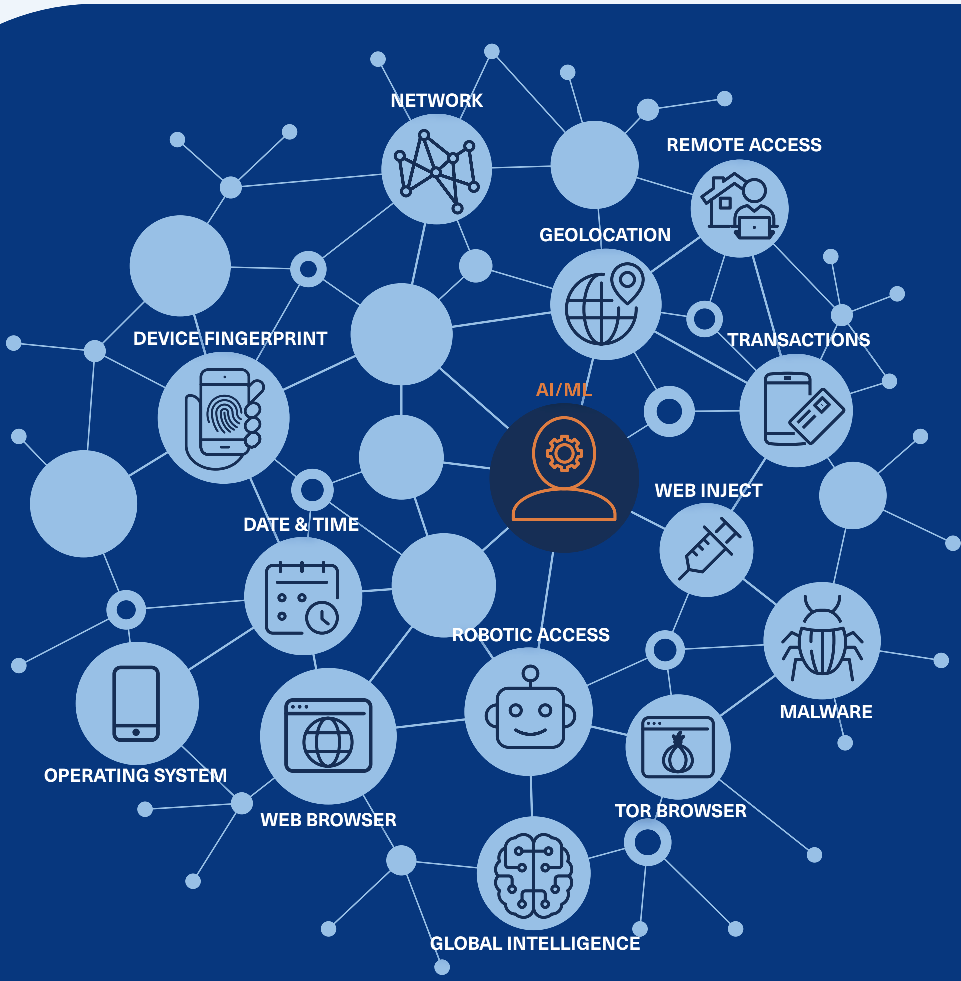
HOW HID GLOBAL USES BEHAVIORAL BIOMETRICS

The primary purpose of HID Global's Risk Management Solution (RMS) is to inhibit fraud by ensuring secure and safe online experiences where legitimate users are easily validated, and fraudsters kept away.

RMS creates a completely trusted user behavioral profile by observing behavioral patterns such as mouse movements, keystroke dynamics, and navigational patterns within the application itself. This data is collected dynamically and unobtrusively via dynamic data collection points in the background of the active application, thus, not affecting the user's experience in any way.

The solution employs technology that gathers and analyzes more than 6,000 features from the way a single user interacts with the keyboard alone. The keystroke dynamics, such as how long one is pressing on individual keys, are amongst the factors used to determine the identity of a user. Using linear discriminant analysis of the keystroke dynamics features, RMS enriches a user's profile, used to authenticate them.

The sophisticated and complex methods analyze the cursor movements of each user on all protected pages within the protected application, evaluating not just the movement directions and speed but also curvature angle and distance. RMS exploits the mouse movement analysis as one of the factors to identify ongoing attacks using, for example, scripted access when fraudsters are trying to break into the application.



The solution applies complex, state-of-the-art machine-learning algorithms to create a user-specific behavioral profile using the multitude of inputs gathered while a customer interacts with the protected application. This profile, continuously updated and improved in real-time, can be used to seamlessly identify a unique user. These markers, augmented with user-specific information such as location, device, time, and navigation patterns, deliver the best context-value resulting in a high fraud detection rate and decreased number of falsely rejected users.

This approach of identifying users through behavioral biometrics is recognized by the European Banking Authority (EBA)[1]. EBA notes that this information, related to physical properties of body parts, physiological characteristics, and behavioral processes (and the combination of these) created by a human body, can be used as an inherence authentication factor.

Meaning that, if properly adopted, inherence provides seamless, frictionless re-authentication without the need for SMS OTPs which has proven to be insecure for years.

The behavioral biometrics-enabled, continuous re-authentication is invisible, happening in the background, improving the user experience for a client who does not need to re-enter passwords or use other means of identification while interacting with the application.

or a complete way to detect and prevent fraudulent activities before they occur, behavioral biometrics also serve as part of HID's wider Risk Management System for ultimate security. Want to learn more about leveraging a complete risk management solution? Read "The Ultimate Guide to Risk Management Systems" now >

Ready to talk to an HID security expert or to learn more about the HID fraud prevention solution? Visit the fraud prevention web hub.

SOURCES & REFERENCES

1. EBA, Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5- 44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

2. EUR-Lex, 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), https://eur- lex.europa.eu/eli/reg/2016/679/oj

3. EUR-Lex, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

4. EDPB, Para 56 of Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0, Adopted on 15 December 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsul tation_en.pdf

5. EUR-Lex, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

6. EBA, Regulatory Technical Standards on strong customer authentication and secure communication under PSD2, https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic- money/regulatory-technical-standards-on-strong-customer-authentication-and-secure- communication-under-psd2

HID
hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108
For more global phone numbers click here

Part of ASSA ABLOY