aimbrain
simply smarter authentication

JAG SHAW BAKER
EXCELLENCE INNOVATION GROWTH

GDPR AND BEYOND:

COLLABORATION, CONSENT, CAPTURE AND CARE IN THE WORLD OF BIOMETRIC DATA

DECEMBER 2017

AUTHORS: AIMBRAIN & JAG SHAW BAKER

Table of Contents

Contents

Introduction 2

The Rise and Rise of Biometrics 3

GDPR and Biometric Data: Key Considerations 4

What are the key GDPR impacts and implications for companies engaged in the processing of biometric data? 4

GDPR and the Role of Consent: 6

Active biometric data capture & consent 6

Passive biometric data capture & consent 7

Beyond GDPR: The Future of Biometric Data 9

The ecosystem 9

The consumer 9

The technology 9

The architecture 10

Best Practice Checklist for Tomorrow's Biometric Partners 10

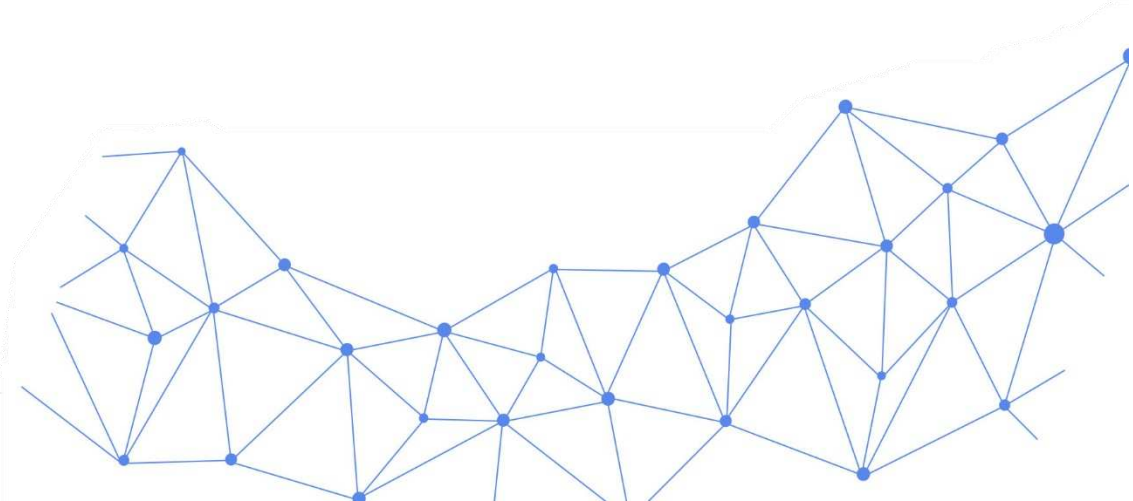
Conclusion 11

About the Authors 13

AimBrain 13

Jag Shaw Baker 13

Key term glossary, according to GDPR 14



Introduction

According to the 2017 Global Trust Barometer issued by Edelman[1], trust in technology and tech organisations has remained relatively stable, but "*people are not convinced that the tech sector is adequately transparent and authentic in how it operates…*[and] *there are also growing concerns about how effectively the sector is protecting their data.*" It appears that whilst we are comfortable enough to share updates and photos across social media networks, there is still an underlying concern about how our data is captured, stored and used by organisations.

And rightly so. Checking in to a market in Seville on Facebook is one thing; a breach that leads to your personal or financial data being leaked on a monumental[2] scale is another. Regardless of the reason for the breach - inadequate security measures, vulnerable storage mechanisms or increasingly sophisticated social engineering - we need to know that organisations, and the organisations with whom they choose to work, are taking more than adequate care of our sensitive information.

Regulation and regulatory change increased by nearly 500% between 2008 and 2015[3], with a key focus on consumer choice (PSD2), and identification (KYC, AML). Both areas seem rather at odds with increasing privacy laws however, with one area driving greater transparency of identity and the other championing consumer choice through the wider sharing of one's personal data through open banking mechanisms. And as if that weren't challenge enough, businesses are now facing the implementation of GDPR (the General Data Protection Regulation), taking effect in May 2018. As successor of the Data Protection Directive 95/46/EC, this new regulation aims to modernise and strengthen EU data protection laws dubbed as the "next-gen data protection".

In this paper, we have teamed up with law firm JAG Shaw Baker to review biometric data usage from a data protection perspective. This paper will focus on:

- The implications of the GDPR on capturing, storing, using, anonymising and disposing of biometric data
- The future of biometric data beyond GDPR, and
- Best practices for biometric data-centric organisations

[1] https://www.edelman.com/post/trust-tech-no-room-complacency/
2 https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/
3 http://uk.businessinsider.com/the-regtech-report-global-regulatory-requirements-are-creating-a-huge-opportunity-for-regtech-firms-2016-8?r=US&IR=T

The Rise and Rise of Biometrics

Since its introduction to corporate use cases in the 1960s[4], biometrics are now commonplace across banking, government, enterprise applications, physical access and more. And now, thanks to the likes of Apple, using fingerprint – and now facial scans - to unlock devices has put biometrics in the mainstream, and the industry is set to be worth an estimated value of $25.3bn by 2020[5]. It is no surprise then that with the widespread adoption of biometrics as personally identifying information, comes greater regulatory requirements to safeguard and protect this data; GDPR.

JAG SHAW BAKER EXCELLENCE INNOVATION GROWTH

*Biometric data, as defined in the GDPR, means: "**personal data** resulting from **specific technical processing** relating to the **physical, physiological or behavioural characteristics** of a natural person, which **allow or confirm the unique identification of that natural person**, such as facial images or dactyloscopic (or fingerprint) data".*

This is a cumulative test and the GDPR rightly clarifies that the processing of certain personal data, such as photographs, should not systematically be considered as biometric data unless such personal data is processed through a specific technical means allowing the unique identification or authentication of a natural person.

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, article 4(14)

From biological samples to fingerprints to emerging technologies such as vein scans, gait scans and even ear canal scans; there are hundreds, perhaps thousands, of ways to uniquely identify each of us. That said, there are just two primary collection methods to capture biometric data:

1) **Active** authentication - by asking an individual to undertake an action, such as providing a fingerprint or facial scan. These are regularly undertaken by many of us - using a thumb or fingerprint to unlock a phone, for example, or looking at a camera to verify your identity when moving through passport control.

2) **Passive** - by capturing or monitoring biometric data invisibly, or behind the scenes. This is not quite as terrifying as it sounds; behavioural authentication - whilst new - is gaining traction as a non-intrusive way to corroborate the physiological patterns of a person with their normal behaviour. Monitoring the speed at which you type, the range of movement you use on a mouse, the angle at which you hold your mobile device; these and many more points can be used to create a unique profile of your behaviour, and provide a reference dataset which can be used to passively authenticate 'you'.

Regardless of what is being captured, and the way it is being done, GDPR recognises the data as a new category of personal information and as such, those involved in the usage or capture of the information will need to abide by new standards.

[4] http://www.springerlink.com/index/M1647W5773136432.pdf
[5] http://www.kezi.com/story/36552207/biometric-authentication-identification-2017-market-segmentationapplicationtechnology-market-analysis-research-report-to-2020

GDPR and Biometric Data: Key Considerations

For many of us, personal information may be in the public domain – on a networking site like LinkedIn, or in a document on a publicly available site like Companies House. But having our biometric data made public would be far less palatable and so even though biometric data is a subcategory of personal data according to GDPR, individuals need to feel assured that the data is extremely well protected.

It is therefore not a huge surprise to see biometric data having new found sensitive personal data status, so let us consider the two most significant impacts for companies involved in the large-scale processing of biometric data; the **immediate implications of GDPR**, and the **role of consent**.

What are the key GDPR impacts and implications for companies engaged in the processing of biometric data?

JAG SHAW BAKER EXCELLENCE INNOVATION GROWTH

The old Data Protection Act 1998 made no reference to biometric data. The GDPR now expressly identifies biometric data as a "special category" of personal data (more commonly known as sensitive personal data under the old regime). Whilst the position on how organisations should handle sensitive personal data has not monumentally shifted under the GDPR, most companies processing biometric data are unlikely to have treated each biometric data set as sensitive personal data and as such will need to reassess their approach in light of processing activities relating to sensitive personal data being subject to greater restrictions and obligations.

Companies processing any type of personal data have always been subjected to specific rules and best practices, but GDPR will bring with it new consequences and higher standards for companies engaged in the processing of biometric data. Some of these considerations include:

1. The obligation to appoint a **Data Protection Officer** (DPO) internally; a position responsible for ensuring "that the data protection rules are respected in cooperation with the data protection authority[6]". This person will be the key liaison with regulatory bodies such as the EDPS and the go-to contact for the application of data protection.
2. Understanding the definitive roles of **data processor and data controller**, and how the roles differ according to the various relationships between an enterprise and any third party or partners that form the ecosystem, as well as infrastructure providers such as cloud servers, network providers and data centres. A biometric data company may hold various processor and controller positions within a single contract, and it will involve significant work to ensure that every part of the chain fulfils its privacy and protection obligations. This could get particularly thorny in the event of a breach or failure at some part; firstly determining the processor and controller roles, secondly the assessment of the impact and finally the subsequent obligations for identifying, containing, auditing and communicating the issue. Being able to determine unequivocal culpability in a dense network of partners could be

[6] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

challenging, and therefore biometrics partners that can demonstrate the seriousness with which they manage additional third-party relationships and security within them will become sought after.

3. Full comprehension of the differentiation of **anonymisation and pseudonymisation** of data; both have different GDPR requirements and repercussions:

    a. **Anonymisation** of data (where the data is stripped of any personally identifying information including the ability to apply any process that could result in the identification of an individual) is subject to far fewer regulations around privacy and the impact of GDPR is limited. An example of this would be collecting blood samples to generate a large-scale survey, in which donors are anonymous.

    b. **Pseudonymisation** of data however is where it is converted into a code, serial number or other identifier, rendering it impossible to identify an individual without applying some kind of process or key. Somewhere along the chain, the data – however innocuous its form – will relate to an individual, and so the onus is on the biometric partner to ensure that the pseudonymisation process takes into account the possibility, impact and likelihood of the threats of today and tomorrow. This is, of course, subjective, and constantly evolving. A good biometrics partner will be able to demonstrate the measures that it takes to render data useless in the event of a suspected breach, and the steps that it takes to ensure that data cannot result in the identification of an individual. One example would be that it insists on contracts that keep its data entirely separate from personal data, and that it can demonstrate the immediate and secure deletion of any information it captures once it has fulfilled its purpose (e.g. authentication for an app or physical gateway).

4. The demands upon it – now and in the future beyond GDPR – of being able to demonstrate the way in which data was collected and used for an individual, if the day comes in which organisations need to be **transparent to the consumer**. This will include how to demonstrate that information was deleted, if requested. This does not just relate to biometrics partners, but to enterprises in general.

5. The challenge of describing all of the above considerations in a clear, transparent and digestible format for the regulator and users. This is particularly problematic when the very processes used involve complex technology based on evolutionary algorithms, neural networks and other schools of deep learning; some, by their nature, independent of human intervention and unrestricted by the limitations of human capabilities of identification and comparison.

These are the initial considerations, and we can only expect the demands on a biometric data partner to grow over time.

GDPR and the Role of Consent:

In the opening sections of this paper, we outlined the two ways in which biometric data is captured: actively and passively. The question of consent forms a critical part of GDPR compliance, and so we ask, from a 'consent' perspective - does GDPR differentiate between passive and active biometrics data capture, or are they equal in the eyes of the regulator?

Does actively providing biometric data, via a facial scan or thumbprint for example, constitute consent?

JAG SHAW BAKER EXCELLENCE INNOVATION GROWTH

Companies must ensure they have a lawful ground for processing biometric data. It has been made clear by the UK Information Commissioner Officer (ICO) that consent is not always the most appropriate lawful ground on which companies should base their processing activities on[1]. However, when it comes to special categories of personal data such as biometric data, organisations may have little alternative as the other lawful grounds for processing sensitive personal data are much narrower than for processing non-sensitive personal data and are unlikely to apply to a large number of companies processing biometric data.

*As such, it is important to ensure that consent is obtained in a way which complies with the GDPR standard of being freely given, specific, informed and unambiguous with **clear affirmative action**. The key to satisfying this threshold is ensuring transparency of how the biometric data will be processed and avoiding any reliance on silence, pre-ticked boxes or inactivity to evidence consent has been given.*

For most companies processing biometric data, consent needs to be obtained in order to use it, and organisations will be obligated under the GDPR to gain explicit consent to use the data and articulate how and for what purpose the data is to be used.

Of course, banks and other users of biometric data will usually have a consent agreement in place when engaging with their customers. Clear and inclusive information on the process and purpose of capturing and using biometric data should be included in an organisation's customer terms and conditions – presented in such use cases as enrolling for mobile banking for example.

For banks, the advent of open banking through PSD2 and the wider fintech movement means that third parties are increasingly joining the ecosystem. Where the third party is privy to, or responsible for, sensitive information such as biometric authentication companies are, they can and should assist in the construction of the consent capturing process, to ensure that the data that they are using is compliant from the controller's perspective.

Needless to say, they must also be compliant in their processes too, by using data only for the purposes notified to the customers, securely deleting data after its use, not storing raw data where possible, pseudonymising or anonymising the data where necessary, and adhering to the strictest security protocols.

JAG SHAW BAKER EXCELLENCE INNOVATION GROWTH

Biometric Identity as-a-Service (BIDaaS) providers are often one step removed from the consent capturing process as this will often be carried out directly by the customer. Whilst the temptation is therefore to avoid getting involved with this process, BIDaaS providers should ensure customers are accurately describing how biometric data will be processed and capture consent accordingly. This should be appropriately covered in the contract with the relevant customer and will help BIDaaS providers demonstrate their compliance with GDPR and fulfil their accountability obligations. Customers should embrace the involvement of the BIDaaS provider in this process, as they will be best placed to describe exactly how the biometric data will be processed and shape appropriate privacy notices.

Conclusion: As with any personal data, the organisation responsible for collecting the data needs to be explicit in the contractual agreement as to the nature and purpose of its processing activities. Contracts need to incorporate clear and unequivocal explanations and gain consent for its usage, and third parties using the data can assist by reviewing or contributing where appropriate.

What about passive biometric data gathering, such as how you interact with an app, for the purpose of authenticating your identity?

JAG SHAW BAKER EXCELLENCE INNOVATION GROWTH

The GDPR does not differentiate between passive and active biometric data capture. Biometric data is broadly defined to not only cover the more obvious physical or physiological traits pertaining to an individual but also expressly includes "behavioural characteristics" of a natural person. This means data captured via passive authentication such as the speed at which you type, will need to be held to the same standard as data captured by active authentication, such as fingerprint data, to the extent it fulfils the criteria contained in the biometric data definition.

Whilst holding biometric behavioural data about a user (such as how they interact with a mouse, keypad or device) could not, in isolation, seemingly identify an individual in the same way a photograph or voice recording could, technically it still is personal information as of course it relates to an individual's record held at the bank or institution. Therefore, the capture and usage of this information needs to also be factored into an organisation's terms and conditions.

The difference between voice or facial biometric data and behavioural biometric data though, is that in order to fulfil its purpose as an identifier, behavioural data needs to be stored for longer and reused, to create an ever-more insightful behavioural identity of an individual in multiple contexts. One swipe of a device is not enough to form the basis of authentication; hundreds of actions contribute to a far more accurate 'picture' of a user, allowing for faster and more accurate authentication.

This raises an interesting question of when such passive data will be deemed to be biometric data. One record of the pressure and speed at which an individual enters a password, in isolation, is unlikely to be information capable of allowing or confirming the unique identification of that natural person.

However, where the profile is built up over time it may be that this passive information alone can identify an individual with increasingly precise accuracy. Would a certain level of accuracy be enough to create a tipping point at which point the data set is elevated from personal data status to biometric data status? This is a fairly simplistic example as in reality biometric data companies will use multiple data sets in combination to identify an individual; however, it suits to raise the point that the broad category of "behavioural characteristics" is likely to cause some issues which the regulators will need to provide guidance on in due course.

Transparency of this sort of activity and notifying customers of this form of authentication will be essential. An area of particular difficulty for biometric data companies will be crafting an appropriate retention policy for this sort of personal data and informing individuals of this policy upfront (especially when it may not be clear at the point of capture how long the data will need to be retained in order to make it useful before it is deleted).

Biometric data companies should also note the plethora of provisions throughout the GDPR which govern "profiling" and the need to make data subject aware of such profiling and the consequences of such processing activities.

The terms and conditions around this data then needs to include information about the ongoing use of this data, and may be obliged to give timescales for its usage and subsequent deletion. This could however prove difficult, as collecting data from one frequent user will be faster than collecting it from a more sporadic user, so the storage times could differ significantly.

Again, third party users or capturers of this data can and should assist organisations in the creation of compliant consent statements in order to adhere to GDPR standards.

Conclusion: Behavioural or passive data, although not as obvious a personal identifier, is just as important under GDPR rules. Enterprises though should be aware of any additional consent required to hold the data for longer than a single use, as behavioural biometric data requires longer to build a more detailed profile of a user. Third parties using the data can and should assist an organisation in ensuring its consent capturing process is sufficient.

Beyond GDPR: The Future of Biometric Data

As we have discussed, there is no single set of rules around the capturing, storing, usage or disposal of biometric data, but we can be sure that as biometric authentication rapidly replaces the use of passwords (something you **know**) and single use pass codes, tokens or hardware (something you **have**) to provide the third factor inherence authentication (something you **are**), regulation around this data will rapidly grow. As such, we have identified some of the potential change that we can envisage.

The ecosystem

Relationships with third party biometrics partners will continue to bloom, as developments in biometric authentication and deep learning algorithms become the default manner to authenticate a user and enable faster transaction times and increasing transaction processing capabilities. Added to this, developments will no doubt lead to cloud-based, centralised digital identities, where open banking and other third-party ecosystems may plug in to a single virtual identity for authentication and verification purposes.

JAG SHAW BAKER EXCELLENCE INNOVATION GROWTH

The Article 29 Working Party (EU advisory body) back in 2012 commented that whilst centralisation of biometric data was acceptable, biometric data should be stored where possible at a device level. However, this opinion does not seem to have survived the passage of time as there is a clear trend to capitalise from cloud offerings and as more start-ups add to this ecosystem with solutions across multiple devices and channels, it seems inevitable that biometric data storage is likely to become more centralised.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

The consumer

As regulation increasingly evolves to protect the consumer, organisations need to consider beyond tomorrow, beyond May 2018. Those engaged in the practice of biometric data processing need to consider that in the future, they may be obliged to show the historic end-to-end audit of the data, so it is imperative that they are focused on their own proprietary data collection and management. A convoluted network of third party modules brought together under one brand or organisation will struggle, so a company that has conceptualised, built, enhanced and fully own its modules will be in a better position to do this.

The technology

Rather than continue to develop ever stranger biometrics to measure, technology should be the enabler. Relationships need to be forged with biometrics fintech partners that are focused on security and the customer experience; those who develop robust but user-friendly biometrics that serve their security authentication purposes but do not compromise the end user experience. It should not be about capturing more, but using what is available in a more sophisticated way.

Biometrics processors should use simple, easy-to-capture biometric data and harness their own expertise and technology to make the data extraordinarily secure and fit-for-purpose. Consumers do not want to provide overly sensitive data, and do not want to rely on hardware or additional software to provide yet another biological trait; blood, ear canals, gait analysis.

The architecture

Finally, biometric data processing should be built on an architecture fit for the future; continually evolving to remain ahead of both the changing cyber-fraud and data breach threat landscape. Organisations, particularly those that have experienced the ever-increasing demands of regulation such as financial services, should draw on their experiences of the past – the resources, time and process overhauls that have overwhelmed and stifled the business' development. The sheer computing power alone required to capture and utilise biometric data, and utilise tomorrow's algorithms is only set to grow, so the cloud will be the only viable option in the future. Legacy financial services providers feel the strain now of trying to retain compliance capabilities in-house; the successors have moved to cloud models and fintech partnerships to bring in expertise and scale.

Best Practice Checklist for Tomorrow's Biometric Partners

With all of the above in mind, we have created a 'Best Practice' checklist for organisations looking to work with biometric data handlers and third parties that use their customers' biometric data. Enterprises should check that a potential partner can fulfil the following best practice guidelines and show evidence that they:

- Pseudonymise biometric data and store in unusable formats such as algorithmically-derived mathematical constructs
- Relate this pseudonymised information to a serialised version of an individual's personal information, not directly against the personal information itself
- Store biometric data away from PII (personally identifiable information) such as name, address, date of birth or financial history
- Securely delete, and ensure the impossibility of regenerating, raw biometric data such as images and voice recordings as soon as it has served its purpose
- Use templates to generate the mathematical constructs, and ensure that these templates are revocable in the event of a suspected breach (so that any data at risk of being compromised is rendered useless)
- Demonstrate commitment to GDPR and privacy through the appointing of a DPO, implementing privacy by design and carrying out privacy impact assessments for new technologies or new processing activities
- Ensure the confidentiality, integrity, availability and resilience of processing systems and services
- Demonstrate the ability to restore the availability and access to captured data in a timely manner in the event of a physical or technical incident
- Document the regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

- In general, show thought to counteracting against likelihood of breach and reconstruction of identity, and be able to demonstrate technical measures in place that consider responses to various types of threat
- Utilise the cloud, to ensure that the scale, technological developments in deep learning and AI are catered for, and the potential future state of the 'single digital identity' is readied
- Ensure that data is stored using the most rigorous of security standards and that regular integrity testing takes place
- Ensure that when information is transferred via Cloud APIs, standards such as TLS 1.2 and API request signing, like HMAC SHA-256 are utilised to prevent attacks
- Use strong encryption algorithms to prevent against attacks between APIs and SDKs
- Ensure that device-based sensitive data such as passwords are securely ring-fenced within the SDK, so as not to transmit or use this data in any way other than anonymous behavioural monitoring
- Become (or work with organisations that are) compliant to certain recognised standards such as ISO/IEC 27001:2013 - Information Security Management System standards and champion the establishment of industry-specific codes and certifications
- Understand the new reporting obligations in respect of data breaches and implement systems to report to data controllers without undue delay in the event of breach

Conclusion

Developments in regulations around the privacy of the consumer will continue to rise, and organisations need to be in a ready state for a biometric-enabled future world. GDPR is putting into place the building blocks to start truly treating biometric data with the respect that the consumer deserves.

Whilst the details of GDPR are currently ambiguous in places, we believe that regulation will not inhibit the use of this highly sensitive data, but will provide the impetus required for forward-thinking, digital-first organisations to consider a longer-term cloud strategy, particularly when considering the rapid rate of adoption of biometrics as authentication as instigated by the end user.

However, as with any industry, Darwinian rules apply and biometrics companies that can display a fundamental, unwavering focus on security, technology and the customer experience will thrive. GDPR will invoke a change to the biometrics market as unprepared or uncommitted companies fall, and with every iteration and new regulation to come, eventually the truly regulation-ready, future-focused biometric partners will remain.

As discussed above, there are a number of areas where further guidance is required in order to fully understand the implications which the GDPR may have on organisations processing biometric data, particularly in respect of how regulators will deal with the broader category of "behavioural characteristics" which falls firmly within the definition.

It should also be noted that whilst the GDPR provides part of the picture in terms of governance of biometric data, each Member State may maintain or introduce further conditions and limitations, with regard to the processing of biometric data. This ability to derogate away from the harmonised GDPR position leaves a piece of the puzzle missing and may make it more difficult for biometric data centric companies to apply a single approach across the whole of the EU.

What is clear is that biometric data usage is on the rise, driven by use through mainstream devices such as iPhones, and there appears to be a real benefit to society from the use of biometric data and an ever-expanding list of use cases in which it can be deployed. The right balance between developing this area and protecting the rights and fundamental freedoms for individuals will need to be struck and key to this will be transparency and effective consent capture processes.

In an earlier article "Biometric Identity As-A-Service (BIDaaS) – The Rise and Rise of Cloud Biometrics[1], AimBrain identified that "the real value of using biometric authentication will be unleashed when organisations move the process away from device, to the Cloud." We suspect the desire for customer-facing organisations to provide a seamless service across multi-channels and multi-devices will fuel the development of BIDaaS.

The likes of financial institutions and large corporations should embrace this movement, question traditional needs of server-side, on-prem solutions and identify partners who are data protection savvy and capable of providing the necessary commitments to satisfy their regulatory requirements. BIDaaS providers who are equally as willing to set the bar in terms of best practice for handling biometric data will take a competitive advantage in this market.

About the Authors

AimBrain

AimBrain is a BIDaaS (Biometric Identity as-a-Service) platform for global financial institutions. Its unique combination of voice, facial and behavioural biometrics with cloud-based authentication authenticates the individual, not just the device. It has the industry's leading cloud-based, multi-module identity authentication solution that combines both passive and active biometrics, and its technology is underpinned by proprietary deep learning, building an increasingly accurate profile of a user over time. Financial Institutions can design a step-up approach to authorisation, escalating through the biometric authentication modules if an initial measurement falls below its acceptance threshold. This appropriate amount of frictions flags fraudulent transactions before they happen. AimBrain is omni-channel, deployed using open-source SDKs, and adheres to best security practices. Visit https://aimbrain.com.

AimBrain is committed to helping financial services companies to use biometric authentication to counteract fraud and improve the customer experience, using the highest security and ethical standards. For further information or to arrange a demo, please contact sales@aimbrain.com.

Jag Shaw Baker

Founded in 2013, JAG Shaw Baker is a strategic law firm that has become central to the European technology and venture capital ecosystem in advising entrepreneurs, companies and investors in high-growth markets including the life sciences, clean tech and digital technology sectors.

We provide a collaborative culture that gives our clients access to exceptional commercial legal advice, deep industry expertise and an understanding of how to build a business from inception through to successful exit. From start-up, scale-up or speed-up to high-growth, late stage, M&A, and post-IPO, our UK and US lawyers have extensive expertise in representing UK and European companies, and representing US and European investors and strategic buyers, on quality transactions.

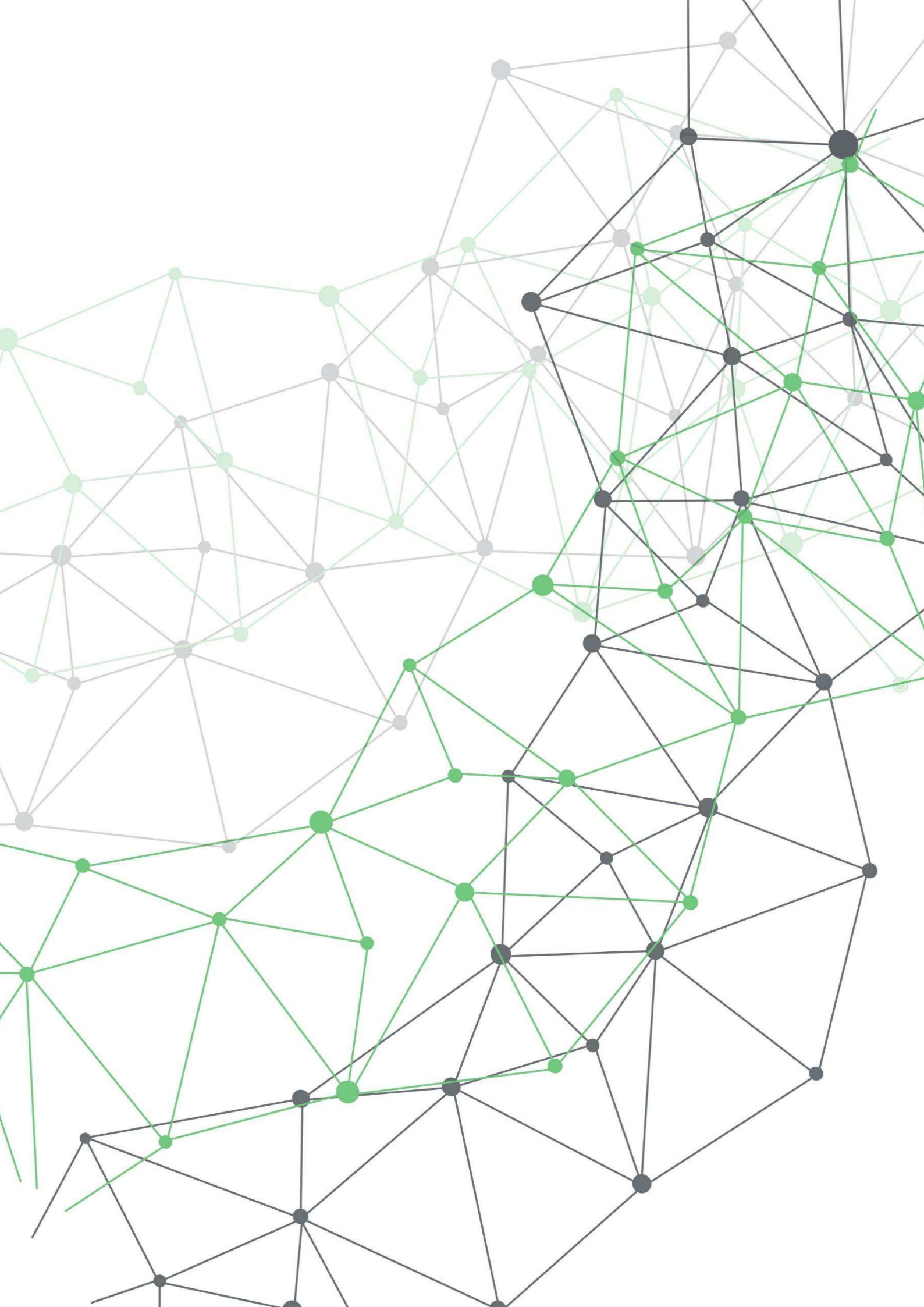
We advise clients on data protection compliance matters, ranging from data audits to complex cross-border data transfers across diverse industries with a particular focus on emerging technologies and software. For further information, please email ashley.williams@jagshawbaker.com.

Key term glossary, according to GDPR

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

'Biometric Data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

GDPR RECITAL 26: The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.