VENDOR PROFILE

Anonos: Helping Businesses Become Data-Driven Without Compromising GDPR Compliance Obligations

Carla Arend Duncan Brown Archana Venkatraman

IDC OPINION

In the digital economy, information is an organization's most important intangible asset. It is the key to personalizing and enhancing customer experience to connect brands with consumers. Organizations that can extract value from their data will be able to use it to open doors to a wide range of new opportunities. They will also be able to differentiate themselves as digital transformation (DX) becomes the norm across all businesses. IDC research shows that 60% of CIOs say their top DX goals are improving customer experience and creating new digital revenue streams, and they see data-driven intelligence as a cornerstone of these goals.

Although data-driven insights can unleash huge business opportunities, businesses worry about not being able to capitalize on the full value of data due to the rigid data protection, security, and privacy regulations that are in place. As we enter a new era of data protection with the General Data Protection Regulation (GDPR), personal data management should be viewed through a new lens, so that businesses can access the technologies that maximize the value of data without compromising their security, privacy, data governance/ownership, or compliance obligations. As data processing and analytics increasingly move to the cloud, ensuring personal data protection is vital for both cloud service users and cloud service providers, as data privacy breaches can have a significant impact in terms of reputational impact and fines.

Data enablement/security startup Anonos is one such company that has developed a new approach to data control, data stewardship, and data protection. Its BigPrivacy platform allows sharing, collaborating, and analytics of personal data while simultaneously enforcing security and data protection policies. It does this by employing pseudonymization technologies such as data de-identification, controlled re-identification and re-linking of data, and a data-centric approach to security. IDC welcomes this departure from existing and well-used techniques such as static tokenization for analytics and data protection because they don't always enable complete data privacy protection and run the risk of re-identification of personal data.

IDC envisages key uses of BigPrivacy, such as GDPR compliance, data collaboration with external parties, IoT data analytics, and processing data in the cloud without jeopardizing compliance. The platform could also help enterprises overcome the main obstacles to cloud adoption and support cloud migration plans.

We believe Anonos' BigPrivacy technology with pseudonymization features and patented technologies will be able to meet latent demand for such technologies as more organizations will want to become data advocates and treat data as a strategic asset while complying with GDPR. It is well positioned to allow analytics and use of artificial intelligence and machine learning on data, including IoT, geo-targeted, and regulated data to help businesses progress in their DX and multicloud journeys. Anonos now needs to invest to raise awareness of its platform and the different approaches to and benefits of pseudonymization technology and its role in GDPR, demonstrate the versatility of use cases, and show how its architecture can scale with data growth.

IN THIS VENDOR PROFILE

This IDC Vendor Profile looks at Anonos, a provider of data management, security, and privacy solutions. The profile focuses on the company's patented BigPrivacy technology, which de-links and pseudonymizes personal data, thereby controlling the linkability and identifiability of data to allow companies to process data for analytics while managing security and privacy compliance. The document also examines Anonos' overall company strategy, go-to-market strategy, market positioning, and future opportunities and challenges within the context of the evolving data protection landscape.

SITUATION OVERVIEW

Businesses that are transitioning from data laggards to data advocates are the ones that will thrive in the digital economy. Organizations are exploring how best to identify, analyze, and use data to enhance productivity and innovate. However, data growth, its fragmentation across multicloud infrastructures, and the tougher data protection regulations such as GDPR are adding further complexities to turning data into business insight. In conversations with IDC, enterprises highlight the trade-offs between the accuracy of analytics and having robust data protection infrastructure. Many believe that the more secure and protected data is, the less sophisticated analytics can be, because it cannot attain granular levels of processing.

This calls for a new approach to data control, accessibility, protection, and security so that the data protection technology acts as a robust framework for secured, sophisticated, and accurate analytics, rather than hindering those analytics.

Company Overview

Anonos was founded in 2012 by Gary LaFever and Ted Myerson, both with experience in data risk management, privacy, legal, and security. Business partners for 17 years, LaFever and Myerson's previous business venture FTEN – a real-time data risk management technology for financial data – was acquired by NASDAQ OMX and integrated into more than 100 stock exchanges around the globe.

It all started six years ago when LaFever and Myerson envisaged the potential value of data and analytics to improve customer experiences and business operations, while being acutely aware of the data privacy and security risks. The duo believed a whole new approach to data control, stewardship, and protection was necessary to unlock the maximum value of data and to turn it into a business asset without violating privacy, security, or regulatory restrictions. With GDPR coming into effect in May 2018, Anonos' BigPrivacy product has found its perfect application.

Their aim was to provide a technology that enables organizations to benefit from data insights derived from analytics and compilation of multiple datasets while keeping personal data secure and private and controlling its access in compliance with current and continually evolving restrictions.

Technology Offering — Anonos BigPrivacy

With six years of R&D and an advisory board comprising legal, privacy, data services, and security experts, as well as executives from heavily regulated industries such as healthcare and academics, Anonos developed its BigPrivacy solution – a scalable, privacy-first focused approach to allow businesses to process data while meeting security and privacy requirements. With five patents for its technology, Anonos' BigPrivacy platform enforces dynamic data-centric security to de-risk data to enable it to be lawfully used, shared, compared, and computed to maximize value. It also facilitates collaboration between two or more parties to have private data inputs to perform analytics on the combined data, with each party only seeing the relevant output and not the full picture to avoid breaching privacy regulations. The objective is to run algorithms on the union of the parties' private data without allowing any one party to view the other party's private data in compliance with privacy, security, and regulatory restrictions. This will become especially relevant with the Internet of Things

(IoT), with the evolving IoT economy producing massive amounts of data but still having to protect fundamental individual rights while gaining significant increased leverage from insights gained from data combined from a multitude of sources.

How BigPrivacy Works

BigPrivacy technology is aimed at enabling data innovation in compliance with privacy, security, and regulatory restrictions. The platform takes source data and converts it into a pseudonymized format that de-identifies data by replacing personal data with tokenized variants. This protects the identity of the data subject, while enabling the use, sharing, comparing, and computing of data between multiple parties.

The key benefit of pseudonymization is that it is possible to re-link tokenized data back to the data subject, but under controlled conditions. By dynamically controlling the link between the pseudonymized data and the data subject, under controlled conditions at individual data level, the platform can help improve the value of analytics without compromising security, data protection, or privacy compliance regulations. Common privacy techniques such as anonymization, generalization, and differential privacy do not allow re-linking of data, which is essential for AI, machine learning, or taking digital transformation to the next level.

Company Strategy

How It Aligns with GDPR Requirements of Data Protection by Design and by Default

Facilitating analytics without jeopardizing personal data and breaching security and regulatory compliance is at the heart of BigPrivacy architecture. The founders decided to take a data-centric approach to security and data protection and build pseudonymization techniques into BigPrivacy. It is interesting to see how the capabilities in BigPrivacy are so well aligned with GDPR requirements.

GDPR

The EU General Data Protection Regulation, which comes into force in all EU countries on May 25, 2018, is shaking up the EU data protection landscape. With GDPR's extraterritoriality clause, the impact extends to all firms worldwide that deal in personal data relating to data subjects in the EU (however transitory).

A key change that GDPR introduces is an explicit emphasis on what's termed "accountability" – under GDPR, this means not only being held accountable for complying with GDPR obligations, but also being able to demonstrate and prove compliance. A major element of this accountability focus is a new requirement, affecting data controllers, for data protection by design and by default (DPbDD).

Infringement of this requirement exposes the controller to a lower-tier regulatory fine of up to 2% of total worldwide annual turnover or €10 million. If there is also a breach of confidentiality or integrity of personal data (a core principle of GDPR), this exposes the controller to a higher-tier fine of up to 4% of total worldwide annual turnover or €20 million.

But what does DPbDD involve, and how will it impact organizations' security measures?

The U.K.'s data protection regulator, the Information Commissioner's Office (ICO), summarizes DPbDD as "a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities" [ICO01].

In more detail, Article 25 of the GDPR states on DPbDD (emphasis added):

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the

> controller shall, **both at the time of the determination of the means for processing and at the time of the processing itself**, implement appropriate technical and organisational measures, **such as pseudonymisation**, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to **integrate the necessary safeguards into the processing** in order to meet the requirements of this Regulation and protect the rights of data subjects.
>
> The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the **period of their storage** and their **accessibility**. In particular, such measures shall ensure that by default personal data are **not made accessible without the individual's intervention to an indefinite number of natural persons**.
>
> An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

The related recital (Rec.78) states (emphasis added):

> "... In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, **pseudonymising personal data as soon as possible**, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, **enabling the controller to create and improve security features**. When developing, designing, selecting and using **applications, services and products** that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations ..."

Anonos began engineering the platform in 2012 when the GDPR concept still only in the minds of the European Commission's data protection stewards. The alignment is certainly a strong positive for the company and a nod to the future-readiness of its technologies and vision of its founders.

The patented technology in BigPrivacy allows the platform to pseudonymize data anywhere from the point of ingest to the data lake, and brings benefits such as:

- The compliant dynamic pseudonymization enables migration to the cloud (see more in the use cases below)
- Offers protection against data breaches by external "bad actors" or misuse by rogue employees because data can be stored and processed in a pseudonymized state
- Meets GDPR's data protection by design and by default standards
- Harmonizes data use and protection against re-identification risk at scale caused by correlations and linkage attacks
- Offers an alternative to consent management by supporting legitimate interest as a legal basis for use

- BigPrivacy ingests data and transforms it into "variant twin" data through pseudonymization, so there is granular control of data, and only necessary data, required for specific analytics tasks, is shared or used (useful for PSD2 banking regulations)
- Provides a means to respect the fundamental rights of data subjects by irreversibly destroying links to demonstrate that a data controller is "not in a position to identify the data subject" as a statutorily recognized alternative to GDPR Articles 15-22 (access, rectification, erasure/RTBF, restricted processing, notification, portability, right to object, automated decision making) – see Article 12(2)

In our opinion, the full enterprise-grade release of the technology with its new approach to data protection couldn't be better timed. Anonos BigPrivacy comes at a time when GDPR is driving interest in new security technologies because it makes data protection a business and boardroom issue and not just an IT problem. Key stakeholders within businesses who are keen to use data as a value creator will influence investment in technologies that help them overcome analytics challenges.

Use Cases

But GDPR is not the only catalyst of BigPrivacy adoption. The technology also has a key role to play in the multicloud era. A cloud migration strategy has become fundamental to digital transformation but there is some reluctance to fully embrace public cloud because of data sovereignty and data security obligations with both data processors and data controllers. In fact, IDC believes, 80% of organizations adopting cloud will commit to multicloud strategies to gain that cloud independence while being able to benefit from the scale and agility of cloud.

- Benefits for cloud service users:
  - Organizations can take advantage of cloud services without fear of breach of data privacy laws, as BigPrivacy pseudonymizes data at the point of ingestion. So, all the data that is uploaded to the cloud is pseudonymized before it reaches the cloud service. That architecture enables organizations to create a global data lake in the cloud and also meet data sovereignty requirements, as the keys to de-pseudonymize the data are held locally in each country and separately to the cloud service (but possibly in another cloud service).
- Benefits for cloud providers:
  - By adding BigPrivacy as a cloud gateway technology, cloud service providers can ensure they are not putting themselves at risk of customers uploading personal data without having proper security and compliance measures in place. As of May 25, 2018, for the first time CSPs will have direct statutory liability (which cannot be negotiated away by contract with data controller customers), as well as joint and several liability with their data controller customers, to protect personal data even if they don't know customers are uploading it (see Article 82). Because only pseudonymized data reaches the cloud service with BigPrivacy, CSPs protect themselves and reduce their GDPR liability.
  - IaaS. Within these environments, providers can guarantee that data is in different regions as the data location can be chosen. BigPrivacy further de-risks their operations by enforcing fine-grained data access and use controls.
  - PaaS and SaaS. These layers from CSPs cannot guarantee that the data is in specific regions, so the advantage of utilizing BigPrivacy is in maintaining or increasing the value of data while also decreasing risk in its stored state. The transition to a variant-twin data set need not disrupt the SaaS or PaaS providers' architecture and can be easily integrated in a gateway or appliance model as an integral part of the fabric of the system and overall process.
- **Protecting data at the edge:** DPbDD can be implemented across all aspects of data use, from point of ingestion to consumption, and never leaving unprotected data vulnerable for longer than necessary.
- **Multipurpose/multidirectional:** Protected processing is multipurpose/multidirectional, rather than single-purpose/unidirectional protection as provided by traditional privacy, enhancing techniques like generalized statistics, static pseudonymization, anonymization, and differential privacy.

- **Protected referential integrity:** Enables controlled re-linking/revealing by separating the information value of data from the means of re-identification (with variant-twin data), protecting against unauthorized re-identification as opposed to referential integrity efforts utilizing static identifiers which are vulnerable to unauthorized re-identification risks from linkage attacks and the "mosaic effect."

FUTURE OUTLOOK

Concerns over data privacy and security have never been stronger, due to the imminent enforcement of GDPR. At the same time, however, the pressure to derive value from data and to take advantage of the scale and agility of cloud services for digital business transformation is extremely high. We are at a point where a root-and-branch change to traditional thinking around data protection, privacy, and security is needed. GDPR compliance is a top priority for organizations, and IDC believes that enterprises will want to invest in a technology that promises to help them maintain compliance without compromising on the value of data, enabling them to execute on their digital projects. However, mere compliance with GDPR does not ensure that an organization can effectively make use of information for analytics – its most important intangible asset.

In our opinion, as the volume, velocity, and variety of data continues to explode in the business world, traditional approaches to data protection will not serve beyond basic compliance at a static level.

In the short term, GDPR will be the primary driving force behind the adoption of Anonos BigPrivacy due to its dynamic pseudonymization techniques that offer data protection by design and by default. In the long run, the promise of sophisticated analytics, a steady migration to the cloud, and the ability to combine multiple data sets in a secure and compliant way will continue to drive the market for data protection solutions built with a unique and innovative approach. With privacy protection laws being implemented around the world, Anonos has a bright future.

ESSENTIAL GUIDANCE

Advice for Anonos

Anonos has developed a scalable, enterprise-grade data protection technology with patented features. Its founders and advisory board also have considerable experience in data protection and security to shape the future of its solution. The vendor is also making progress in building an ecosystem of technology providers (such as Hitachi Vantara) and channel partners as part of its go-to-market strategies. We have the following advice for Anonos:

- In the short term, it needs to improve awareness of the benefits and challenges around different pseudonymization techniques and how it directly aligns with the requirements of DPbDD in GDPR. IDC data shows that investments in GDPR-related technologies for traditional security and storage will peak between 2017 to 2019, and Anonos is well positioned to make the most of this window of opportunity if it can raise awareness levels. This window will continue to grow with the explosion of sensors and devices, with IDC estimating worldwide spending on the Internet of Things to reach $772.5 billion in 2018 and $1.1 trillion in 2021.
- It needs to demonstrate through high-profile use cases how large multinational enterprises have used its BigPrivacy platform to turn data into a business asset but at the same time maintain regulatory compliance.
- It also needs to highlight the benefit of supporting public cloud migration strategies because cloud adoption is a much wider discussion point than GDPR and it can help Anonos establish its value to different personas within an enterprise – security, digital business units, CIOs, cloud architects, and compliance teams.
- Anonos should also target the CSPs, so they can provide a compliant cloud offer. This would provide Anonos with a broader total addressable market (TAM), but it needs to demonstrate that its technology can be baked into CSPs' offerings without significant issues and can enhance the value proposition of the CSP.

- Lastly, it needs to maintain the momentum of innovation and engage with businesses about the broader digital transformation and IoT-related value it brings to the table.

LEARN MORE

Related Research

- *Western Europe GDPR-Driven Enterprise Mobile Security Software Forecast, 2017-2021* (IDC #EMEA43029517, September 2017)
- *Western Europe GDPR Impact on Security Services and Software Forecast, 2016-2021* (IDC #EMEA42677317, August 2017)
- *Western Europe Storage Spending Forecast, 2016-2021: Impact of GDPR* (IDC #EMEA42894616, August 2017)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com