looker

What GDPR Means for Your Business's Data Strategies

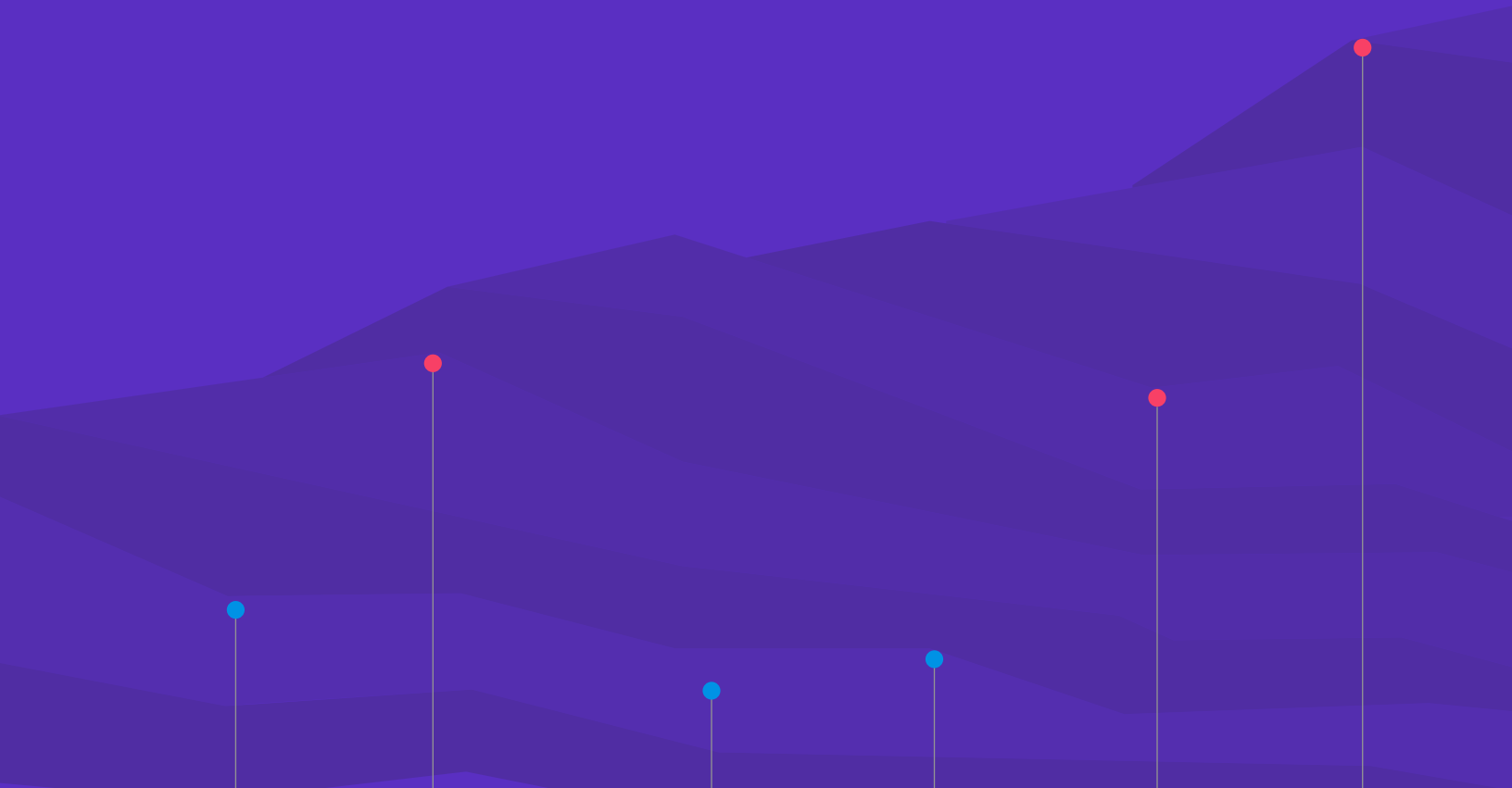


Table of contents

02 Business Data Strategies in the Age of GDPR and Beyond

03 What is the GDPR?

04 Three Thematic Data Best Practices in the Age of GDPR

06 A GDPR Compliance Checklist & Requirements

07 Looker's GDPR Checklist

10 Looker's Architecture Helps Keep Data Secure & Private

Business Data Strategies in the Age of GDPR and Beyond

The General Data Protection Regulation (GDPR) represents one of the most comprehensive reforms to data regulation in recent times. It affects how companies around the globe approach their strategies for external data protections (like data security), as well as internal data access and usage. The purpose is to give EU and UK individuals more transparency and control over their personal data. Additionally, it modernizes and consolidates the data protection rules of individual EU Member States under the previous EU Directive into a single regulation.

The regulation was passed by the EU in April 2016, and went into effect in May 2018. Companies or organizations who collect, use and retain personal data and fail to meet or maintain GDPR compliance can face steep fines, ultimately costing up to 20 million Euros or 4% of global revenue, whichever is higher. The first fines from GDPR violations were issued before the end of 2018, with even more likely on the horizon.

More than just avoiding monetary penalties, organizations across industries also have an opportunity to appeal to consumers worldwide as a champion of consumer privacy through GDPR compliance.

2 in 5

of consumers say they are more comfortable and confident that brands are handling their data correctly thanks to the introduction of the General Data Protection Regulation (GDPR) in May 2018.

Source (DMA UK, Jan 2019)

It is important to not only meet regulatory requirements, but to leverage the opportunity to drive brand and business value. The key starting point is to understand the fundamentals of GDPR compliance and form a strategy that allows you to better manage data.

> “When privacy is done right, that knowledge will bring customers confidence and trust in the vendors who demonstrate respect for their data. Privacy is good for business—and for innovation. Achieving this takes expertise, experience, commitment and engagement across organizations. Technical, legal, and business teams must collaborate to make this a reality.”

Barbara Lawler
Chief Privacy and Data Ethics Officer, Looker

What is the GDPR?

The GDPR is a set of regulations designed to protect EU individuals' personal data and expand their rights to control its use. It requires companies to have effective data governance through the data lifecycle.

In turn, both businesses and people can exist in a safer, more predictable society where data is safeguarded by universal rules and regulations, and is intended to enable the EU Digital Single Market. For the foreseeable future, GDPR will continue to be a challenge for businesses to fully operationalize.

While the GDPR is European in scope and culture, its influence extends to other countries around the world that are seeking to establish data privacy regulations of their own. It is important to keep in mind that no single country or region owns the rules. Each country interprets privacy according to its cultural norms and legal frameworks. Other international efforts, along with legal data protection regulations and frameworks in 126 countries and across 50 U.S. States, prove that responsibly handling people's data is serious and critical for business success.

What is Personal Data under GDPR?

Personal data under the GDPR means "any information relating to an identified or identifiable natural person ('data subject')," which is a person 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."

In layman's terms, personal data is information from, about or derived from or can locate an individual. These personal identifiers can include name, email address, mobile number, device identifier, location information, health information, financial account and credit card information, income and cultural profile.

What are the GDPR Penalties for Non-Compliance?

Companies that fail to meet or maintain GDPR compliance standards do so at the risk of incurring large monetary penalties. Per the fine print in the new regulation, there are a variety of sanctions that can be imposed for non-compliance. If it is your first offense, you might receive a written warning alerting you of the non-compliance, as it may have been unintentional.

Three Thematic Data Best Practices in the Age of GDPR

Now more than ever, the importance of data security and privacy for businesses cannot be understated. There are news stories seemingly every week about companies potentially misusing or improperly securing personal data. Large scale data breaches have left consumers vulnerable to identity theft, creating both a public violation of trust and more scrutiny from governments. The lack of transparency surrounding secret or inappropriate uses of personal data are negatively affecting the trust relationships between individuals and business. Data security and privacy protection are vital to the success of every organisation.

If you're looking to modernize how your business uses data to be GDPR compliant, there are three thematic pillars of data security and privacy to consider: data governance, data centralization, and monitoring data and access.

1 Data Governance

Data governance involves the people, processes, and technologies required to create a consistent and proper handling of an organization's data across the business. Companies must maintain current documentation of their data supply chain from time of collection to erasure, such as data flow maps and data inventories. This includes the technologies used, accountable staff, and documented policies that are operationalised: what data is collected, why it is collected and how it will be used, where that data lives, how it's secured, how access is controlled and how it will be erased when requested or has expired.

Start the process of organizational data governance by understanding and documenting your data supply chain:

- Firstly, **identify what data is being collected**. Then, understand why it is being collected and its planned uses; consider unanticipated uses. Transparency about the types and intended use of personal data is essential and must be published in privacy policies and communicated to the individual at time of collection.
- Identify the **minimal amount of data that you need**. Determine what data is to meet the defined purposes described previously. Is it an email address? An email and a phone number? Or, an email, a phone number, a mailing address, and credit card information? Is any of the personal data considered to be part of 'special categories' under GDPR? This will be different for every organization and industry.
- Take a **look at which third party vendors (processors and subprocessors) might access or 'touch' the personal data in your data supply chain**, make sure that they are GDPR compliant, and hold them contractually responsible via a Data Processing Agreement.
- **Understand and document where all personal data is stored**, including how it will be protected to prevent both internal and external security breaches. This can become extremely complex if employees or vendor technologies extract, export, copy, locally store data on their servers, computers, thumbdrives, cloud storages, etc.
- Finally, put in place and document a retention and deletion policy, including **processes to erase personal data** after a designated time (subject to other legal restrictions), or upon request by the individual.

2 Data Centralization

Companies are amassing data at exponential rates with the expectation that more data will improve analysis and business decisions. At the same time, they are creating a fundamental issue called 'data sprawl.' This is when the same data lives in multiple locations, and across multiple systems and types of data sources. Data sprawl can easily undermine the ability to understand and document all locations where personal data lives and the ability to effectively analyze it.

Increasingly, companies are turning to cloud solutions, such as Google BigQuery, Snowflake, Microsoft Azure or Amazon Web Services. Centralizing an organization's data is the most efficient way of documenting where data lives and is used, while providing the capability to substantially increase data analysis effectiveness and speed. Centralized data also reduces overall security risk, such as fewer attack vectors and more streamlined means to securely access data, while leveraging the performance benefits of modern database technologies.

Data centralization can presents a win-win business situation: more easily documentable data supply chain for GDPR compliance and provides increased business efficiencies in the process.

3 Monitoring Data and Auditing

Monitoring data and data access make up the third pillar of GDPR compliance. This ties with who has access to personal data and why the data has been collected and will be used by your organisation. Once you've set controls about who — both internal and third party vendors — can have data access and why, you can then monitor to prevent unauthorized access by individuals, and make sure they are not improperly accessing or misusing personal data. Having the ability to monitor and review logs of data access will help maintain the integrity of your organization by establishing greater accountability.

If an incident or breach involving personal data does occur, GDPR regulations require that businesses put processes in place that determine and document who has been affected and the risk to them. GDPR compliance also requires that regulators be notified within 72 hours and that individuals whose data has been breached are notified without undue delay. A centralized database creates event logs of data access, and a platform like Looker can streamline that process by revealing which user accessed what data in a faster, more efficient way to meet strict SLA (Service Level Agreements).

If the data was instead stored in a more centralized and flexible data platform – meaning employees no longer need to extract data to analyze it – the risk and potential impact of a leak like this is minimal. In addition, staff can interpret data more quickly and act on it directly, accessing only the data they need to answer their immediate questions."

John O'Keeffe
VP EMEA, Looker

A GDPR Compliance Checklist & Requirements

> “The reality is maintaining GDPR compliance for the foreseeable future requires a shift in mindsets when it comes to data. This is a long-term process and one that businesses must stay on top of. Organizations now must approach data with the mentality of ‘what business problems we are trying to solve with this data?’, rather than ‘if we can store it, we may as well do so’ - and some still need the help of experts and tools to understand what information they can leverage for decision making, what’s useful and what’s not.”
>
> John O’Keeffe
> VP EMEA, Looker

Compliance will never be achieved, only maintained.

GDPR compliance is not a project that can ever be completed; it’s an ongoing process requiring a blend of people, process, and technology that will continue to evolve over time. As your business continues to grow and change, it will be necessary to add or remove technology, people and processes to better serve your data needs. GDPR is forcing companies to rethink how they collect, store and use personal data throughout the data lifecycle.

The following GDPR compliance checklist not only helps you understand GDPR requirements, but also offers actionable steps to take in order to execute those priorities.

Looker's GDPR Checklist*

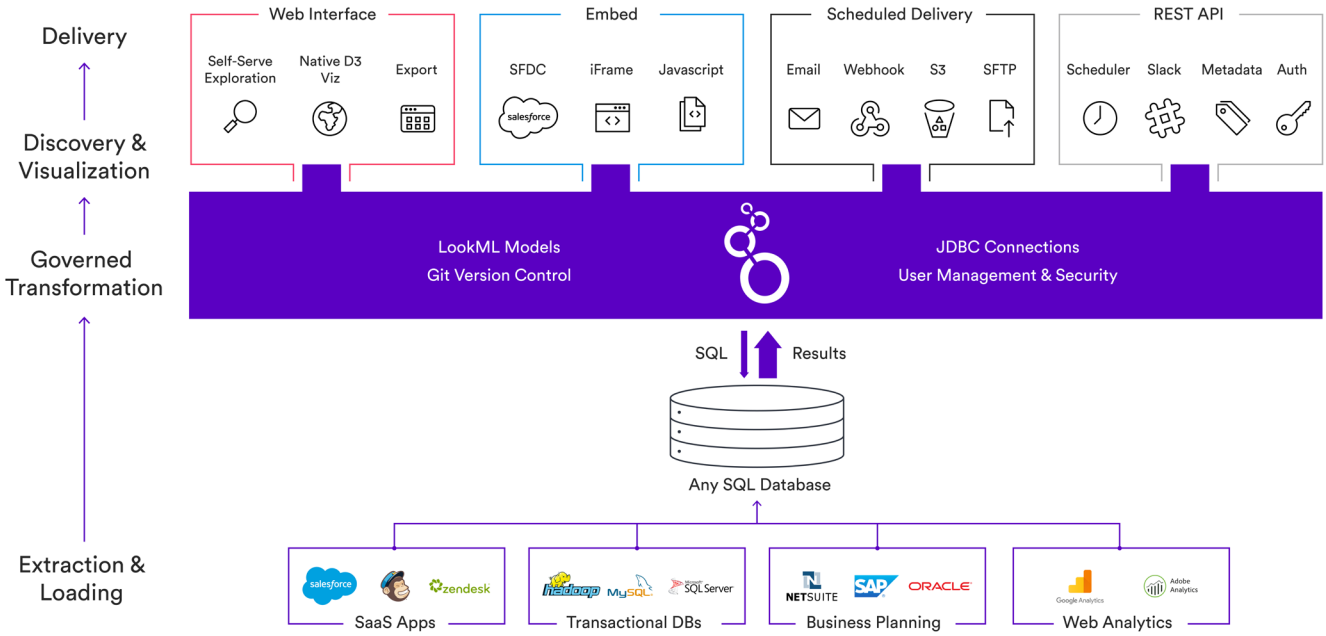
*Please note: The GDPR is a complex set of regulations, and every company's approach to GDPR compliance will be unique. Companies should work with their own advisors to determine how best to comply with the GDPR requirements. More information about how Looker complies with the GDPR can be found on our website.

REGULATION PRINCIPLES	WHAT THIS MEANS	HOW LOOKER CAN HELP
Data Governance and Privacy Design	**Audit, map and document your data supply chain**: the personal data that flows into, throughout and onward to third parties. Describe what data and its sources, the purposes and uses, where it is stored, and how are you protecting it. The documentation should include: • Details of the processing of all personal data. • Legal basis of processing of all personal data (e.g. fulfillment of a contract, legitimate interest, consent). • Details of any transfers to third parties and third countries (who and where, technical and administrative controls in place). **Identify any gaps or weaknesses in your data supply chain** that could lead to misuse or compromise of personal data. For example, use of a third party vendor that has not met GDPR compliance requirements, or discovering personal information living locally on business user laptops. Plan to perform a Data Protection audit annually. Data protection audits and data mapping are part of a comprehensive privacy program lead by a privacy professional.	Looker is a 'Data Processor' to its customers, which are the 'Data Controller'. We have a privacy program in place designed to meet GDPR compliance requirements. The responsibility for processing personal data consistent with a GDPR legal basis lies with the business. Looker has user and role-based permissioning that allows for each authenticated user to only see the appropriate data intended for them. Data Models can be designed that a user with no assigned access can default to no data access, thus eliminating weaknesses in the supply chain. Additionally, Looker performs regular third party penetration tests against the Looker application and hosted environment in order to ensure data protection. Looker also makes it easier to: • Understand the data you have collected. • Implement a simpler architecture for data processing. • Select regional Looker-hosted or if necessary, on-premise. • Have the ability to govern access to data at the database, model, group and user level. • Better understand transfers of data to third party systems managed via Looker's monitoring and audit functions. **Audits can be easier with Looker**, since there can be one access point for users to work with your business' data. If that data is centralized, only one version of that data could exist. This makes it easier to track who accessed the data, and when they accessed it.

REGULATION PRINCIPLES	WHAT THIS MEANS	HOW LOOKER CAN HELP
Data Hosting and International Data Transfers	When dealing with international data transfers, GDPR requirements set specific restrictions and administrative requirements on data transfers outside of the EU to unapproved jurisdictions for both data processors and data controllers.	Looker provides clients with a variety of hosting options to help meet GDPR compliance standards. We can host your platform in a secure, single-tenant cloud in several geographies and cloud hosting providers around the world. Additionally, Looker participates in the EU - U.S. Privacy Shield and applies the EU Standard Contractual Clauses (SCCs) for data transfers outside of the EU.
Data Accuracy and Retention	**Data Accuracy** • The GDPR requires that personal data be gathered for specific purposes only (as described in the Data Governance section). • Companies are required to keep personal data accurate, current, and maintain its integrity. **Data Retention** • Personal data that is collected and retained should not be retained longer than is strictly necessary for the defined purposes, and be evaluated for the proper retention period, minimizing the length of time it is retained. Retention schedules should be set and implemented when data expires. • Management or actions relating to data deletion must include an audit trail.	**Data Accuracy** • Looker's model can monitor every database interaction. This functionality allows administrators to audit usage, and easily set up reports and alerts. • Your data model is both global and version-controlled, which allows users to access the same data, and track when metric definitions have changed, who changed them, and why. **Data Retention** • Alerting functionality allows administrators to automatically receive reports on upcoming expiring data or set webhooks to create automated processes for data that needs to be expired.
Automated Decision Making and DPIAs	The GDPR sets controls and safeguards for profiling individuals and automated decision making about individuals or groups of individuals. Profiling and the application of robust analytics and algorithms, machine learning and AI require companies to conduct a Data Privacy Impact Assessment (DPIA) to evaluate the risks to individuals and determine the specific means to mitigate those risks, including human intervention and building robust anonymization techniques into data engineering and data science processes. Individuals have the right to object to profiling and challenge decisions and actions based on algorithms.	Looker only accesses the data in a way clearly defined in the version-controlled and auditable modeling layer. Looker can be used to anonymize data for downstream automated processing. Analysts can build fields in Looker that abstract the data in the presentation layer without changing the data in the database itself.

REGULATION PRINCIPLES	WHAT THIS MEANS	HOW LOOKER CAN HELP
Securing Data and Breach Obligations	One of the main tenets of GDPR is to have in place the appropriate technical and organizational data security measures. High up on your GDPR checklist should be Encryption and Pseudonymization. However, there are some caveats when it comes to encryption: • Encrypted data is designed to become decryptable, only if you have the key. • Managing encryption keys properly involves overhead (and some risk). • Encrypting personal data may mean further processing is not possible. • If you don't need it in its original form, consider hashing as that is non-reversible. • Pseudonymisation is a de-identification process, replacing personally identifiable information fields with one or more artificial identifiers, or pseudonymization. **Breach obligations**. In the event of an incident or breach involving personal data, organizations are required to notify their lead regulator within 72 hours in order to be compliant with GDPR requirements, and to individuals without undue delay, even if you have incomplete information about the incident.	Looker uses hashing, encryption, and key management controls to protect your data. **Data at Rest Protection** • Native Looker username and passwords are secured using a dedicated password-based key derivation function (bcrypt) with hashing and salting. • Customer database credentials and cached query results are stored using AES encryption via centralized key management provided by AWS's KMS, Customer instances utilize unique keys. **Data in Transit Protection** • Data in transit is encrypted from the user's browser to the application via TLS. • Looker enables you to configure your database connection via SSL or construct an SSH tunnel.. The Looker SOC 2 Type 2 report is available on request to potential customers under an NDA. **Breach obligations**. Leveraging Looker's technology, it can possibly assist in identifying the source, scope, and breadth of a breach in order to report it to regulators and individuals within the required time frame.
Rights of Individuals (Data Portability)	A key principle of GDPR compliance are 'enhanced rights' for individuals regarding their personal data, including access and correction, and data deletion and portability. These rights take precedence over the needs of the data controller. • In the case of personal data deletion, it must be removed from every location, including third party systems, unless other legal restrictions apply. • Organizations must keep an audit trail of personal data access, correction, deletion, or portability requests and actions taken.	• Looker architecture ensures less data sprawl, making it easier to find the personal data subject to data access, correction or deletion requests. It facilitates more precise erasure of personal data. • Looker's UI or API can be used to locate personal data in a centralized database and deliver it in a variety of commonly used electronic formats. • Looker has built a personal data deletion capability that allows the administrator to delete a Looker user's account data. We have an internal engineering process to anonymize the data.

Looker's Architecture Helps Keep Data Secure & Private



Your Data Stays in Your Control

Looker enables data availability, as opposed to data storage. The Looker platform's 'in-database processing' design means transformations occur at the centralized database level at the time of query, with no data being extracted or moved. To enhance the performance of regularly queried data, found on dashboards for example, Looker has a short-lived cache that is cleared after 30 days or when it reaches 2 gigabytes. Customers can also set their own cache time limits to be shorter or longer. The data remains in your control.

Data Governance from the Bottom up

The architecture of Looker inherently lends itself to GDPR compliance when it comes to data governance. A robust modelling layer allows for granular levels of data governance. Administrators have the ability to set granular permissions by user or group, and to restrict data access all the way down to a column or row. This allows different users to only utilize data they have permission to access directly from the database. Reports sent to those without appropriate permissions simply won't see that data. By connecting to a centralized database, Looker provides a single point of data access, and everyone's data access is fully governed.

Comprehensively Monitored & Fully Auditable

Using Looker to explore or monitor a database activity log reveals who has accessed what data and when. And if sensitive information is breached, Looker can help identify who and when it was accessed. Understanding data access allows for greater accountability when it comes to meeting data security and privacy regulations. Data access monitoring and auditing becomes more simplified with Looker.

> What's unique about Looker is that it's a centralized data platform that leaves customer data in their databases. This means that people no longer need to extract (make copies) data to analyze it. They can interpret it and act on it directly within their browser, accessing only the data they need to answer their immediate questions, while still retaining the ability to ask more."

Barbara Lawler
Chief Privacy and Data Ethics Officer, Looker

Enterprise-Grade Security Feature Set

Looker's **Soc2 Type 2** compliant data platform is equipped with enterprise-grade features like two-factor authentication, SAML-based single sign-on (SSO), and team management to keep access to Looker data safe and up to date. Looker also uses industry-standard AES encryption to secure your database connection credentials and cached data storage. We take data security and privacy very seriously, so Looker uses TLS to encrypt network traffic between our platform and user's browsers.

Partner with Industry-Leading Consultants

Looker has technology and consulting partners around the globe who can help develop and implement data strategies and roadmaps that work best for your organization.

Version 1, who contributed to this paper, is a consulting partner based in Ireland and UK with over 1,000 employees. They are trusted by global brands to deliver IT services and solutions which drive customer success and GDPR compliance.

About Looker

Looker is a unified Platform for Data that delivers actionable business insights to every employee at the point of decision. Looker integrates data into the daily workflows of users to allow organizations to extract value from data at web scale. Over 1,600 industry-leading and innovative companies such as Sony, Amazon, The Economist, IBM, Spotify, Etsy, Lyft and Kickstarter have trusted Looker to power their data-driven cultures. The company is headquartered in Santa Cruz, California, with offices in San Francisco, New York, Chicago, Boulder, London, Tokyo and Dublin, Ireland. Investors include CapitalG, Kleiner Perkins Caufield & Byers, Meritech Capital Partners, Redpoint Ventures and Goldman Sachs. For more information, connect with us on LinkedIn, Twitter, Facebook and YouTube or visit looker.com.

About Version 1

Based in Dublin, Ireland, Version 1 proves that IT can make a real difference to our customers' businesses. We are trusted by global brands to deliver IT services and solutions which drive customer success. Our 1,000 strong team works closely with our technology partners to provide independent advice that helps our customers navigate the rapidly changing world of IT. Our greatest strength is balance in our efforts to achieve Customer Success, Empowered People and a Strong Organisation, underpinned by commitment to our values. We believe this is what makes Version 1 different and more importantly, our customers agree. Learn more at version1.com.