STRONGLINK

EU's New GDPR Privacy Rules Are Impacting Global Companies

Are You Ready? Learn How It May Affect Your Data Management Strategy

These are tough data management laws, which will immediately apply to any company that does business in Europe.

It is no illusion that every time you turn around it seems there is another report of a high-profile hack of sensitive personal data, impacting hundreds of millions of people all over the world. The recent Equifax hack released personal financial data of over 143 million consumers, but that was not an isolated incident. In 2016 and 2017 so far there have been at least 26 major hacks around the world that have released personal data of more than 700 million people. These include hacks of telecommunication companies, financial institutions, government agencies, universities, shopping sites, and much more.

The hacks are not a new problem. But in a global economy with often conflicting political and economic priorities at stake, there has been no comprehensive approach to ensuring people have the right to protect, and delete if they want, all of their personal data.

This is about to change as the European Union's new GDPR (General Data Protection Regulation) comes into effect in May 2018. Although GDPR is designed to protect European citizens, the rules and penalties apply to any company from any country who does business in Europe. And the penalties are significant, with companies at risk of being fined up to 4% of their global annual gross revenues or €20 million (whichever is greater) for failing to comply with strict right-to-be-forgotten and privacy protections for customer data.

As a result, there is a growing panic among businesses as they try to figure out how to solve this problem in time, and how to do so with existing data management and storage resources that are not designed for this task. And the concern is not only in Europe. Companies in the US and around the world who have customers in Europe are also scrambling to ensure they are in full compliance by the deadline. But according to Gartner, by the end of 2018 over 50% of companies affected by the GDPR worldwide will not be in full compliance with its requirements.

In this paper we offer an overview of the key provisions of GDPR that impact storage and data management for both structured and unstructured data. In subsequent technical briefs, we will go into more detail about specific technical solutions to help ensure your data environment is in compliance, even with your existing storage and data infrastructure.

European Union's New GDPR - Privacy Rules with Teeth

The objective of GDPR is to protect EU citizens' personal data and privacy. Personal data includes data such as name, address, email, social media, phone numbers, credit cards, transactions, buying history, website visits, browser history, etc. All organizations that do business in the EU or with EU citizens are required to comply with this new regulation no later than 25 May 2018. Make no mistake, this is a regulation with enormous teeth. Compliance is not optional. And it completely and radically changes how business is conducted with the EU. Take the example of sending an unsolicited email to attend a webinar or seminar, receive a newsletter or just to start a sales call; EU citizens cannot be automatically "opted in" for emails, newsletters, updates, or anything else. They must first give permission. That permission must be documented and easily produced on demand. And that's one of the easier requirements to meet.

GDPR is critically important to companies from any country that have European citizens amongst their customer base. It specifies roles, processes, and technologies that are required to comply in making EU citizens' personal data secure, accessible, appropriately utilized, with documented consent. The 88-page document laying out the requirements and obligations under GDPR is linked at the end of this paper.

"By the end of 2018, over 50% of companies affected by the GDPR will not be in full compliance with its requirements." Gartner.

Meeting all of the GDPR requirements will be difficult and in some cases extraordinarily so. Failure to comply will risk severe financial consequences as further detailed at the end of this document.

This is where StrongLink brings significant value. StrongLink is one of the very few products that enables IT organizations to manage most of the really thorny GDPR compliance requirements such as the very problematic right to be forgotten and other provisions noted below.

Why Do I Need to Create a GDPR Strategy?

Complying with GDPR is essentially about finding the proverbial needle across possibly multiple digital haystacks. But not only finding it, but also deleting and proving that you've deleted such data. The problem gets more complex because an individual's personal data may reside in a combination of structured and unstructured data stores, each of which presents different challenges. As if this isn't bad enough, add the fact that deletions must also include all instances of the EU citizen's personal data that have propagated across multiple incremental backup images and which might be stored in archives or DR environments, which usually span multiple different storage types and locations.

All of these different touch points present tremendous challenges for IT organizations who must provide a global solution across them all without crushing IT staff with multiple manual procedures. Unless organizations can globally manage these requirements across heterogeneous data types and storage infrastructures, the risk of missing something and incurring penalties is extremely high.

At the core, GDPR compliance hinges on three key components, all of which are core capabilities of StrongLink:

- **Find it → Data classification:** Aggregating multiple metadata types across otherwise incompatible data and storage systems enables IT administrators to automate searches across any local or cloud storage platform in a single operation. This is particularly important for isolating GDPR content across multiple instances of unstructured data.

- **Delete it → Automated Storage Resource and File-copy management:** This applies to structured and unstructured data, so IT staff can certify that all instances of a file have been deleted, and that such deletions are propagated across all redundant copies on any storage type, including local, remote, and cloud. Since StrongLink manages metadata, data, AND storage resources, deletion policies can be globally applied across different storage types, including cloud.

- **Prove it is deleted → Audit trails and cross-platform reporting:** It is not good enough to just delete the data. Because of the severe penalties, IT organizations need to assure themselves and be able to prove to others if challenged that the GDPR content is truly gone. StrongLink solves this problem with built-in cross-platform reporting capabilities. StrongLink's immutable audit system keeps track of all file actions, using the same metadata engine used to isolate and delete the GDPR data. In this way customers can verify that all instances of an EU citizen's personal data is truly gone.

Which GDPR Provisions Concern Me?

The GDPR regulations are laid out in an 88-page document, which is linked below. This is complex legislation that is an aggregation of at least 27 different privacy regulations that have been evolving in parallel since 1980 in different European countries. The key ones in the GDPR law to think about are noted below.

The Highly Problematic GDPR Article 17 "Right to Be Forgotten"

GDPR Article 17 states that an EU citizen's personal data must be completely deleted for each of the following circumstances:

1. Upon the citizen's request.
2. The purpose for which the data has been collected is no longer necessary.
3. Or user consent has been withdrawn.

In each case all of the personal data and any copies of that data must be deleted. This includes structured data sets, and all of their incremental backups, as well as any GDPR content that might be in unstructured data sets.

Here is why it's problematic: Consider that the vast majority of personal data will be part of a database. Finding and deleting that data from the database is a generally a straightforward exercise using existing database utilities. The problem is with the backups. To delete an EU citizen's personal data in a single backup copy is an annoyance, but is still manageable. Unfortunately, there are many more backup copies than just one. Database backups are generated daily and kept on average 90 days or longer. Even if the database is backing up in an incremental mode, there will be a lot of additional manually labor-intensive work.

Most backup administrators will incorrectly assume that if they recover the original baseline database and then delete the related data, it will be deleted from all of the incrementals and they'll be done. They are only partially correct. Each incremental backup also points at the data in the original. Deletions will cause pointers to break causing errors and likely corrupted backup copies in the versions based on incremental variations.

The conventional way to delete the EU citizen's data from the backups is to recover each incremental backup starting with the most recent, then work backwards to the origin point. Each recovery must be re-backed up after the data is deleted. That's a minimum of 90 database recoveries to delete a single individual's personal data 90 times. It realistically will be many more than a one individual asking to be forgotten, which repeats this onerous process for each and every one. It becomes an unworkable non-trivial task. That task becomes exponentially more difficult when there are four, six, 12, or more backups every day. The right-to-be-forgotten requirement then becomes an impossible nightmare.

The StrongLink Advantage

StrongLink's intelligent policy-based ability to create multiple copies on writes completely changes the game, by providing continuous data protection. Instead of multiple incremental backups, StrongLink converts a database backup into a transparent asynchronous copy. It converts a database recovery into a mount point. That's it. No recovery, just mount the database. Instead of recovering each and every backup copy or virtual copy of the database sequentially and then deleting the EU citizen's personal data from each copy, the database application merely has to mount the master database copy. It then finds and deletes the EU citizen's data from that copy one time. StrongLink policies then can automatically propagate the deletions to ALL copies and versions. There is no recovery process period. There is no additional process to backup once again each backup copy of the database. StrongLink reduces the right-to-be-forgotten compliance into a simple highly automated process.

StrongLink solves this very problematic right-to-be-forgotten provision of GDPR.

Managing Consent – Article 6

GDPR requires that collecting data from its citizens must have a defined use case for the data. In addition, the EU citizen must consent up front, that consent must be documented, and the consent documentation must be provided on-demand by EU regulatory authorities. Proof of consent must be retained. As previously discussed, when the specified use case comes to an end, all of the EU citizen's data must be deleted unless other compliance requirements supersede GDPR.

The StrongLink Advantage

StrongLink automatically harvests, organizes, and parses metadata on all files that are under management. StrongLink also enables admins to automatically apply custom metadata tags to flag GDPR-impacted data -- a prerequisite in order to make sure any EU citizen's personal data is locatable when not in a database. StrongLink additionally maintains data & metadata provenance -- an immutable audit trail that accounts for the data origin together with an explanation of how and why it got to its present place -- that expedites consent management. All of these capabilities make it appreciably easier to locate and track GDPR consent documentation regardless of where it's stored, even if the documentation is in multiple filers, object stores, or the cloud.

Data Protection by design & default – Article 25

Data protection must be built-into the processes and tools that collect European citizens' personal data.

The StrongLink Advantage

StrongLink is purpose-built to provide continuous data protection, driven by global policies across all data stores. The built-in immutable audit system, plus point-in-time versioning ensure that data is always protected. This includes file copy management across any storage type, whether primary, DR; onsite and offsite; private and public clouds; even cold storage including tape or optical. StrongLink data protection is by definition built into the processes and tools that collect EU citizen personal data.

Security of Processing – Article 32

Implement a security level appropriate to the risk including the use of pseudonyms, aliases, and encryption. Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services. Restore availability and access to personal data quickly in a "timely manner" following an outage or failure. Make sure there is a process for regularly testing, assessing, and evaluating effectiveness of these processes.

The StrongLink Advantage

Even though "in a timely manner" is open to legal interpretation, StrongLink meets or exceeds this requirement because data availability is always instantaneous even if one or more of the underlying storage silos has an outage. By leveraging StrongLink's ability to create and manage multiple copies of the data in different storage systems and sites, the data is always available to applications and users regardless of which copy is accessed. Its self-healing architecture is designed for always-on operations

Data Minimization – Article 25

GDPR requires collecting and keeping as little personal data as possible for the minimum amount of time. The retention aspect will have to be balanced with other regulations on keeping records for longer periods of time such as health and criminal records.

The StrongLink Advantage

StrongLink retention and deletion policies are set by the administrator based on numerous variables including application, specific time frames, data age, or other metadata variables. Data can also be migrated between different storage types over time to more closely align data value with storage performance and cost. Policies are fully automated and can be set to retain files or objects only as long as necessary, triggered by one or more metadata tags. StrongLink's intelligent policy engines facilitates compliance with GDPR as well as other regulations, and prioritizes and/or alerts when there are conflicts.

State of the Art (SOTA) – Articles 25 & 32

GDPR requires it be future proofed against ongoing IT technological advancements. This means organizations must either deploy the latest technologies in order to meet GDPR requirements or justify why it did not implement them based on cost, risk, and context. Organization adherence to SOTA must be reviewed regularly.

The StrongLink Advantage

StrongLink is purpose built to connect any storage type, including otherwise incompatible filesystems or storage platforms, ensuring that customers are always free to select the storage type/vendor that best suits their business requirements now and in the future. As existing infrastructure is replaced over time, and new technologies emerge, StrongLink enables customers to focus on their business, knowing that their GDPR strategy is sound regardless of the storage type they have now or may acquire in the future.

Data Transfers - Articles 44-50

This is a GDPR cloud service provider specification; EU citizens' personal data should be stored in EU countries or countries such as Canada that have similar data privacy protection. However, if that data is stored or transferred to countries such as the USA, binding corporate rules that match the GDPR must be in place.

The StrongLink Advantage

StrongLink automatically classifies all data by aggregating multiple metadata types into a common management platform, it means administrators can set global policies to ensure any data is stored where it should be, and excluded from where it should not. These policies can be automatically triggered by metadata, which includes GDPR-specific tags, and which can automate data placement, protection, and accessibility. In a StrongLink deployment that spans multiple sites/countries, such policies will automatically ensure that GDPR data is only stored in locations that comply with the law.

StrongLink reduces the GDPR compliance burden into a simple highly automated process.

Reporting Brings it All Together

A final important StrongLink capability is its immutable audit log and cross-platform reporting capabilities that can automatically generate compliance reports across multiple locations and storage silos. Automated system reports identifying all copies of specified GDPR-related files for a given user or group can be run before and after a compliance run across all storage types and locations to ensure the data is truly deleted.

Such reports have previously been focused on providing a cross platform analysis of storage utilization, project charge back, or other metadata-driven variables. For GDPR, such reports provide a global, actionable view across all your storage silos/locations.

Conclusion

The GDPR compliance date is rapidly approaching, and it is so pervasive that other countries around the world with strong trade relations with Europe are looking to adopt similar measures to ensure they are not at a competitive disadvantage. Larger companies are already searching for GDPR strategies they can use within their existing infrastructure, since compliance is not an option for organizations doing business in the EU or with EU citizens. Failure to be compliant can be financially ruinous.

According to Gartner, however, ''By the end of 2018, over 50% of companies affected by the GDPR will not be in full compliance with its requirements.''

Unfortunately, achieving GDPR compliance using traditional methods is a manually labor-intensive non-trivial task. StrongLink streamlines and automates processes that make GDPR compliance simpler and attainable without a complete overhaul of existing infrastructure or business processes.

GDPR Fines & Penalties

GDPR is a new EU regulation that will quite likely go to through major changes as implementation shows what will and will not work well in the real world. The gears of bureaucratic regulatory change grind slowly. In the meantime, GDPR imposes stiff fines for non-compliance.

Determination

The following 10 criteria will be used to determine the amount of the fine on a non-compliant firm:

1. **Nature of infringement:** number of people affected, damage suffered, infringement duration, & processing purpose.
2. **Intention:** whether infringement is intentional or negligent.
3. **Mitigation:** actions taken to mitigate damage to data subjects.
4. **Preventative measures:** how much technical and organizational preparation previously implemented to prevent non-compliance.
5. **History:** Past relevant infringements, which may be interpreted to include infringements under the Data Protection Directive (predecessor to GDPR) and not just the GDPR, and past administrative corrective actions under GDPR, from warnings to bans on processing and fines.
6. **Cooperation:** how cooperative the organization has been with the supervisory authority to remedy the infringement.
7. **Data type:** what types of data the infringement impacts.
8. **Notification:** whether the infringement was proactively reported to the supervisory authority by the organization itself or by a third party.
9. **Certification:** whether the organization had qualified under approved certifications or adhered to approved conduct codes.
10. **Other:** other aggravating or mitigating factors may include financial impact on the firm from the infringement

Fine Amount

If an organization infringes on multiple provisions of the GDPR, it shall be fined according to the gravest infringement, as opposed to being separately penalized for each provision. However, this may not offer much relief considering the potential fine amounts.

Lower Level Fines

Up to €10 million, or 2% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements of:

- Controllers and processors under Articles 8, 11, 25-39, 42, 43
- Certification body under Articles 42, 43
- Monitoring body under Article 41(4)

Higher Level Fines

Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements of:

- The basic principles for processing, including conditions for consent, under Articles 5, 6, 7, and 9
- The data subjects' rights under Articles 12-22. Note: "Right to be Forgotten" is Article 17.
- The transfer of personal data to a recipient in a third country or an international organization under Articles 44-49
- Any obligations pursuant to Member State law adopted under Chapter IX
- Any non-compliance with an order by a supervisory authority

The many requirements and obligations under GDPR are linked here in the 88-page regulation document: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf