arcserve®

VIEWPOINT

Data Management for General Data Protection Regulation (GDPR) Compliance

By Christophe Bertrand, VP of Product Marketing

Historically, personal data such as name, address, phone number, date of birth, sex, age, and ethnicity have been collected with consent as individuals filled out forms, booked holidays, bought tickets and entered competitions. But with the advancement of social media, smart phones and cloud applications, personally identifiable information (PII) can be collected in far more indirect ways. For example, your IP address and location can be captured from your phone while at a cafe during a coffee break.

All too often, individuals have little to no insight into the scale and breadth of how their data is being collected, analyzed and shared. Ultimately, this explosive combination of ever-growing personal data collection and the sharp increase in data loss incidents has led to robust new regulation designed to protect personal data.

With the rapid rise of technological capabilities and the borderless nature of the modern digital economy, governments have had to adapt to provide better data protection and improve the fundamental rights of their data subjects. On May 25, 2018, the world's most sweeping data privacy regulation, the European Union's General Data Protection Regulation (GDPR), will become law.

The GDPR gives EU residents the right to request from organizations whatever data is being stored about them and to withdraw consent of its use, effectively ordering its destruction. Per Article 12 of the GDPR, this request must be free of charge, easy to make and must be fulfilled without "undue delay and at the latest within one month."

The regulation aims to harmonize the 28 member states of the EU and encourage organizations to be more accountable, transparent and responsible for the data they hold. Any entity that stores or processes the personal data of EU residents will be obligated to conform to this new law, regardless of where that organization resides. Further, it empowers EU residents to control the data that an organization may hold on them.

The EU has given organizations until May 2018 to implement this new law, as most organizations require significant time and investment to support GDPR-mandated processes and capabilities. Given the GDPR's scope and transformative impact, it is important that organizations examine the way they handle personal data.

Non-compliance will be met with fines of up to 4% of global turnover or €20million, whichever is greater.

In effect, the equation has been flipped – instead of choosing to simply pay penalties versus becoming compliant, organizations much now invest in GDPR-readiness or be subject to significant fines.

The GDPR requires comprehensive reform and prompt action with key mandates to follow:

- Accountability and Governance – Maintain relevant documentation on data processing activities and implement measures that demonstrate compliance, such as audits.
- Storage Limitation – Personal data may not be kept for longer than is necessary for the purposes for which it was originally obtained.
- Breach Notification – A notifiable breach must be reported to the relevant supervisory authority within 72 hours of the organization becoming aware of it.
- Individual Rights – An individual may request the deletion or removal of personal data when there is no compelling reason for its continued existence.

Arcserve will specifically call out, among these mandates, the need for data protection and data loss prevention. IT infrastructures must leverage state of the art technology to prevent data loss events.

Today, there isn't one solution that solves all aspects of GDPR. Many different facets affect IT and data-related processes including backup and archiving.

Implications for Backup and Archiving

GDPR Article 5 sets out the key principles for data protection and describes how organizations process personal data, how it may be stored and how it should be safeguarded. Article 5 states that organizations may maintain backup and archive copies of data if the data is processed in a manner that ensures appropriate security of personal data.

Article 5 of the GDPR requires that personal data shall be:

> (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes;
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's data protection requirements. The new Accountability Principle in Article 5(2) requires organizations to demonstrate that they comply with the principles and states explicitly that this is their responsibility.

(a) Implement appropriate technical and organizational measures that ensure and demonstrate that you comply.

(b) Maintain relevant documentation on processing activities.

(c) Where appropriate, appoint a data protection officer.

(d) Implement measures that meet the principles of data protection by design and data protection by default.

(e) Use data protection impact assessments where appropriate.

Arcserve Uniquely Meets GDPR Requirements

GDPR demands improved data governance for backup and archiving. Legacy backup and archiving products are oriented around individual data management challenges, therefore lacking the capability to deliver a comprehensive GDPR solution. Arcserve has taken a unique approach to delivering a robust set of products that meets the needs of broader GDPR-related requirements.

There is an expansive process that is required to define what constitutes personal data in your organization. Obvious areas where you'd find it include databases, emails and workstations. Personal data is defined rather broadly to include personal email, email addresses and other data an organization would collect not only as part of its marketing and business activities but also as part of a normal backup and data protection process. GDPR requires consent from the owners of the data at the time of its collection. In essence, backup copies and emails contain personal data that places another burden: organizations must manage all backup copies and archive email, per GDPR rules. Backup copies are made to save backup data offsite in the event of a disaster. It is common for organizations to have a dozen or more copies of each backup.

When organizations store backup data of inhabitants of the European Union, the backup should reside in the European Union and the backup copy jobs, tapes or cloud copies should be there unless you have a system where the customer has given you permission to store it outside the EU

Organizations that maintain email archives need to pay close attention to GDPR rules. It is common for email archives to store email for years due to business requirements, regulatory requirements and legal holds. In the event a user withdraws consent, an administrator requires standard tools provided by the archive solution to identify emails and remove them from the archive. Activity logs are necessary to keep a record of the destruction as proof for audits.

With current backup technology, there is no way to remove personal data from backups regardless of the vendor.

- It would also open up the risk of massive fraud if you can make an individual easily "disappear" from all live and archive/backup data
- It would conflict with compliance rules that favor the retention and/or the immutability of data

You are allowed to have personal data in your backups, even if the individual has exercised the right to be forgotten. BUT… you are not allowed to do a restore of that data (unless there is a legal reason, such as a lawsuit).

- Per GDPR compliance, personal data stored on backup copies is marked as disposed and cannot be restored once a user withdraws consent
- If you have to do a restore that includes personal data that is supposed to be forgotten, then you'd have to erase it again
- There is consensus that the right to be forgotten applies to live/production data vs. archive or backups

Data in general, including backups, has to be protected from breach (encryption for example). Arcserve solutions have such capabilities.

If you store data that is considered to be personal or sensitive, such as customer data, then the data of European Union nationals (the backup) should reside in the European Union (location)

It is fair to say that at this stage, GDPR creates a number of grey areas for organizations and vendors alike. Interpretations and precedents will help in the future as it gets implemented.

Arcserve Unified Data Protection (UDP)

Arcserve delivers enterprise-grade data protection capabilities without the complexity often associated with enterprise data protection solutions. Small and over-stretched IT teams easily safeguard cloud, virtual and physical data by protecting to and from any target, while configuring and managing all aspects of data protection through a single, elegantly simple user console. As business needs change or requirements evolve, IT teams easily turn on high performance capabilities without burdensome forklift upgrades or layering on additional point solutions.

A key GDPR requirement, as stated in Article 5(2) is that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

From a compliance perspective, regular backup and recovery testing and reporting on protected data is a good way to demonstrate to your Data Protection Officer (new role) that you are in compliance and effectively protection/safeguarding your data.

Arcserve UDP can help with this:

- Standard reports document what backup run, what data is protected and where the data is stored
- Retention Policy reports document how long backup copies are kept and when they are destroyed
- SLA and Assured Recovery reports document the safety of the data, including how frequently the data is protected and how long it will take to restore a backup copy.

UDP Benefits

Improved data protection, recovery and availability

- Unified architecture that brings core data protection technologies under one console
- Feature-rich solution supporting a wide variety of environments
- Customized protection plans to help meet specific data protection needs
- Advanced reporting to demonstrate compliance with GDPR principles

Improved operational efficiency

- Administrator's efficiency is enhanced with Arcserve's unified management console
- Ease of use and broad capabilities combine to enhance time to value
- Storage and network resources consumption mitigation

Improved capabilities to demonstrate compliance with GDPR principles

- Encryption protects backup copies to safeguard data per GDPR rules
- Flexible recovery options manage backup copies for GDPR compliance
- Retention options support long term retention, legal holds and defensible disposition
- Ability to test, measure and report recovery processes for GDPR compliance

Arcserve UDP Archiving

Arcserve UDP Archiving enables organizations to easily meet challenges associated with email search, compliance and legal risk with a purpose-built solution that supports on-premise, private and public cloud deployments. Small and overstretched IT teams optimize operational efficiency and reduce costs by configuring and managing all aspects of their data protection and archiving strategies through a single, elegantly simple user console.

As a new solution within Arcserve UDP, the email technology provides all the tools to help users manage archive email for GDPR compliance. It supports a multi-tenant architecture, giving multi-national and decentralized organizations the ability to separate archive email by location, division or department. For example, email created in a European country can be managed and stored separately from email that originated in North America.

Arcserve UDP Archiving is a purpose-built email archiving solution designed to manage email for regulations such as GDPR, and offers multiple standard controls to respond quickly to GDPR opt-out requests.

When individuals withdraw their consent, administrators use built-in eDiscovery tools to quickly search, identify all emails sent or received by the individual. Remember that this has to be done without creating conflict with compliance requirements. The GDPR regulation is not necessarily clear about this.

Arcserve UDP Archiving Benefits At A Glance

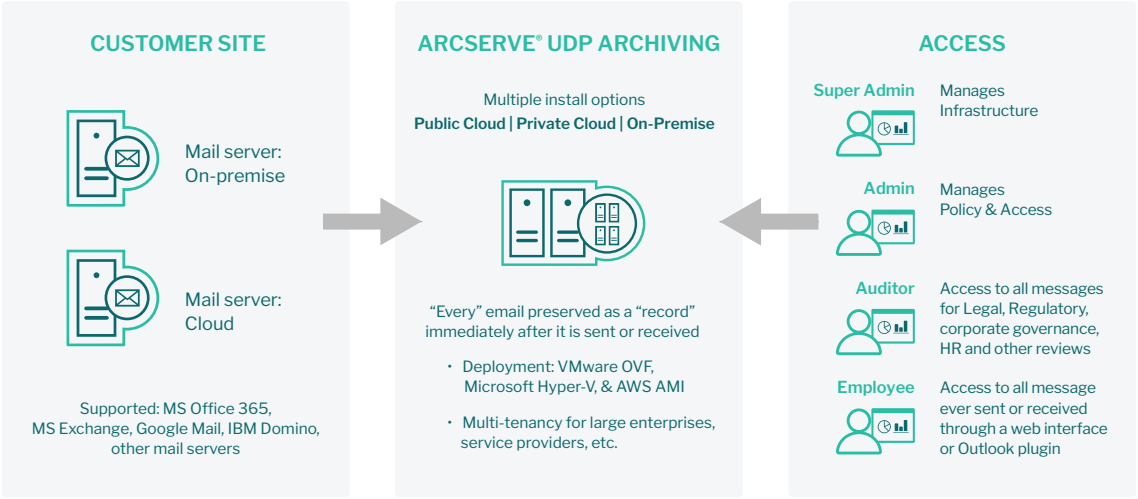
Single-console administration of archiving, search and retention

Fast, powerful search

Multi-tenant control by department, division or location

No limit on number of mailboxes per search

Arcserve UDP Archiving Topology



Conclusion

The GDPR gives EU residents the right to withdraw consent and order the destruction of their email and other personal data, giving way to a new landscape of compliance requirements that organizations must adhere to. While the right to delete personal data has been emphasized by many, it is only one of the aspects of the regulation. It is also clearly focused on the protection of personal data, which affects operational backup and recovery decisions.

The teams charged with managing backup and email data require robust, yet easy to use tools that allow them to quickly identify personal data and remove it from their systems. Arcserve UDP and its archiving solution deliver the capabilities needed to demonstrate compliance with GDPR principles, including backup and recovery from a central console, granular recovery with the ability to exclude files, and full activity tracking and reporting to demonstrate compliance.

In the event a user withdraws consent; an administrator can quickly identify personal archive email using standard tools. Arcserve UDP and its Archiving solution are an important part of ensuring a resilient GDPR strategy. Arcserve is currently developing additional capabilities across its portfolios to further support GDPR compliance. Please contact our teams for more details on our solutions

For more information on Arcserve, **please visit arcserve.com**