Lanmark Limited - epicbackup^{TM} Service
“Right to be Forgotten”

The arrival of the European Union's General Data Protection Regulation (GDPR) is imminent: the official cutover date is 25 May 2018. One question requires special attention for backup data: the “right to be forgotten”.

According to the GDPR, a data controller (the person or organization processing the data) is required to offer the right to erasure, also known as the right to be forgotten under certain circumstances, to data subjects (a GDPR-specific term for individuals).

When an EU citizen invokes his or her right to be forgotten, a data controller must erase all of the personal data that it possesses about that person. But a grey area immediately becomes apparent: if a controller is using various processors (such as third-party cloud data storage providers), and some of the data subject’s personal data is being stored by that processor, who is responsible for its deletion: the controller (who originally captured and handled the personal data), or its processor(s)?

The controller clearly must respond to ensure that an individual can exercise his/her personal data rights, which include:

- access (being able to see what the controller and its processors have collected on the person)
- rectification (requesting corrections to any errors
- restriction of processing
- portability
- erasure

Any processor the controller uses is also required to assist with “appropriate technical and organizational measures” to help it honour the data subject’s rights.

An individual has the right to request erasure of his or her personal data if:

- The data is no longer necessary for the purpose for which it was collected
- The data subject withdraws consent to processing, and there is no other legal ground for processing, i.e., the controller cannot demonstrate an overriding legitimate basis for processing
- The processing is otherwise unlawful.

These are the only circumstances under which a controller is obligated to honour a data subject’s request to be forgotten.

Beyond primary data: the right to be forgotten and data backups

When users exercise their right to be forgotten, they likely expect that any backup copies of their personal data will be erased as well. This presents a technical challenge to controllers and processors. First, an individual's personal data might be scattered across many applications in a company (e.g., CRM, marketing automation, order entry, etc.) and distributed across several on-premises data stores and/or in the cloud. The backup associated with each application might reside in separate archives. Further, every backup archive typically includes data from many other applications and users.

Usually the original files and backup archives are organized and built in a way that makes it impractical to delete an individual's personal data entirely without affecting the backups of other applications and users. Deleting one user's data could adversely affect the protection of many others users' data – effectively negating the point of performing data backups in the first place.

Balancing competing obligations

As a data protection company, Epicbackup is obliged to preserve backups even in the wake of erasure requests. We operate a global network of data centres in which we store backup archives on behalf of our customers and partners. But Epicbackup has no visibility into what type of data is stored in these backups, personal or otherwise.

Even if we assume that most backup archives contain personal data that is subject to erasure requests, there are many cases in which Epicbackup cannot allow modification of the backup archive due to contractual or legal obligations to our customers and partners. In some cases, this is a reflection of the inherent function of backup: to enable the restoration of lost or damaged data from an exact copy that was made at a specific point in time. In other cases, we must preserve backup archives because our partners and customers may be relying on them to honour their own regulatory or legal obligations.

For example, they may be relying on perfectly preserved backups to satisfy e-discovery requests in an ongoing lawsuit, or for compliance with some industry or tax regulation regarding records retention. In those cases, the GDPR recognizes that personal data from backups cannot be deleted immediately in response to a user's request for erasure because other concerns take precedence over it.

Responsibilities after recovery

Keep in mind that the primary responsibility for honouring the right to be forgotten remains with the controller. Since restoring a production system from backup could reintroduce that previously removed data, controllers must take steps to ensure that data is again deleted from the production system after recovery.

Honouring a user's right to be forgotten in backup archives comes down to two questions:

- How can we protect that data while it continues to persist in a backup archive?
- How can we honour GDPR's principals of data minimization, keeping only the data we need for the minimum amount of time we need it?

Best practices for handling personal data

Epicbackup has several GDPR compliance best practices and product features designed to help customers (businesses that serve as controllers of EU citizens' personal data) to honour this obligation:

- Where possible, controllers should organize backups so that each data subject gets his or her own separate backup archive for personal data.
    - This is an ideal solution because it enables the granular deletion of personal data without affecting the records of other users.
    - Unfortunately, this approach is likely to be impractical for many businesses to implement, as an individual's personal data is often scattered across multiple applications, locations, storage devices, and backups.

- Backup archives should always be stored using strong encryption. That way, even if a backup archive with personal data awaiting deletion were stolen, the thieves couldn't use it.

- When individuals request the erasure of their personal data, controllers should be transparent with them about what will happen to the backups:
    - Primary instances of their data in production systems will be erased with all due speed
    - Their personal data may reside in backup archives that must be retained for a longer period of time – either because it is impractical

to isolate individual personal data within the archive, or because the controller is required to retain data longer for contractual, legal or compliance reasons.

- The individual can be assured that their personal data will not be restored back to production systems (except in certain rare instances, e.g., the need to recover from a natural disaster or serious security breach). In such cases, the user's personal data may be restored from backups, but the controller will take the necessary steps to honour the initial request and erase the primary instance of the data again.
- Backup archives containing personal data will be protected with strong encryption, so that even if criminals were able to steal the archive, its contents would remain useless to them.
- Retention rules have been put in place so that personal data in backup archives is retained for as short a time as necessary before being automatically deleted.
- Records of all data subject requests regarding their personal data will be retained, as will audit logs that record all activities on backup archives containing personal data. This means that the user can be confident that their personal data has been backed up in accordance with GDPR principles of security by design and by default, as well as data minimization, and that their rights, including the right to be forgotten, have been honoured.

How Epicbackup honours the right to be forgotten when we are the controller of personal data

Epicbackup will honour the rights of all data subjects regarding their personal data, including the right to be forgotten, when the data is no longer needed for its original purpose or the user withdraws their consent. When a customer asks Epicbackup that he or she be forgotten, we will delete their personal data (e.g., name, surname, mailing address, telephone number) from our production systems within 30 days if there are no legal grounds for processing it further.

We will delete backup copies of that personal data from our archives as soon as is practically possible, to the extent allowed by our other data retention obligations (e.g., to protect other data stored in the same backup archives, or meet other regulatory or legal requirements). As soon as those obligations have been fulfilled, we will permanently delete those archives as quickly as possible.

Epicbackup will also retain audit logs showing the history of all operations on the customer's personal data for the period required by legal obligations. Certain items the user might consider personal data, e.g., entries made on community discussion boards or review pages may be retained according to the Terms of Service that the user agreed to when they posted. Epicbackup will always take reasonable steps to keep all personal data secure and inaccessible to unauthorized individuals.

Conclusion

Whether you are a controller, a processor, or both in GDPR terms, honouring a data subject's right to be forgotten is pretty straightforward: if it resides in your production systems, you need to delete it swiftly. But that same data copied into backup archives can be a little trickier to handle: you need to delete it as soon as possible, but may have other obligations to preserve it for longer.

The best way to avoid a potential compliance violation and the stiff fines that come with it is to follow the same general GDPR principals for backups as you do for personal data in production systems:

- Take reasonable steps to keep backup archives safe and secure from prying eyes
- Don't hold onto archives any longer than you absolutely have to
- Log and document your policies, procedures, and actual operations on backup archives so you can prove you've acted in good faith to honour data subjects' rights regarding their personal data stored in backups
- Be transparent with users about why their personal data in backups might be kept around longer, how you will keep it safe until it can be deleted, and when its eventual deletion will occur.