Backup and GDPR, what is the relationship?

The General Data Protection Regulation for the protection of personal data states that the Data Controller, taking into account his specific **operational** context (purposes of processing, categories and number of data subjects involved and personal data processed) and the related **risks** for the rights and freedoms of natural persons, must implement technical and organizational security measures in line with personal data and processing activities.

For this to happen, three essential elements of personal data must be protected by the organisations;

- **confidentiality -** data are available only to the persons authorised to process them**;**
- **integrity** – data must not be altered, deleted, or unduly modified;
- **availability** – data must be available when required.

So, what is the relationship between backups and the protection of personal data?

As mentioned above, the organisation shall protect not only personal data confidentiality but also their integrity and availability; backup is essential under GDPR, as it is one of the most important security measures that can be taken by organisations.

Let's start from defining what a backup is: a backup is the process of **making copies** of information and personal data in accordance with a scheduled time frame and is an important tool to **maintain the integrity and ensure the availability of personal data,** which could be compromised in the case of violations coming from outside but also as a result of **operational errors, failures, or natural events** (accidental data deletions or changes, failures that render archives unusable, application errors, fires ...).

Without a consistent backup strategy, the organization cannot recover data that have been unduly deleted or modified.

A backup file is a copy of data files (or applications, systems, etc.); we will not go into more technical details about full backups, incremental backups or system snapshots; any decision about “how” and “when” depends on the context and requires a specific design (as an application of the Data Protection by Design principle – article 25 of GDPR).

A **data breach** is often associated with the unauthorized disclosure of personal data, so with the loss of their confidentiality. This is probably the kind of data breach that scares the most, but it is not the only possible one.

Just imagine a company that, accidentally or as result of a targeted attack, becomes the victim of a ransomware that encrypts all the data it owns: in this case, the data have not been disclosed outside but are simply inaccessible and the company is requested to pay a fee in order to have its own data back.

The data still reside within the systems but in an encrypted form, being unavailable to the legitimate users: this is also a data breach. If the organization can rely on a valid backup, the previous system configuration and user data can be made accessible again. Therefore, the backup turns out to be an extremely important security measure to protect personal data.

Organizations should carry out their own backups in a structured way; the methods for making security copies should be determined according to the **context and be consistent with the service delivery policy** adopted by the organization itself, defining the so called ‘backup strategy’ (backup type, interval, time and mode of recovery, retention period, number of backup copies and place of storage) adequate to its specific needs (Article 25 relating to ‘Data Protection by Design’ and Article 32 ‘Security Measures’).

When developing their backup strategy, policies and tools, the organizations need to take in account the following aspects:

- Copies should not be **physically located in** the primary company premises but in a different location (off-site). An adverse natural event – such as fires, earthquakes, flooding – could be a serious threat for the company and a backup copy stored in the primary location may go lost or damaged along with the systems under backup, causing that way an irreversible loss of data integrity and availability.
- Data recovery tests should be **carried out periodically** to ensure that everything is working exactly as expected.
- Once the **retention terms of personal data have expired,** the backup copies that contain them must be deleted and not stored further.

Data retention and backups have a complex love-hate relationship.

Backup is an important and crucial activity for the IT security but also a challenge for personal data protection, since the backup copies may contain personal data. When the data retention period expires, the organization must delete personal data from the systems – a relatively easy task. But what about the personal data stored in the backup media? Targeted deletions within backups are still possible in theory but in turns out to be quite a daunting task in a real operational context. So, almost always, organizations keep personal data until the backup retention deadline expires, and such kind of deviations must necessarily be managed by organizations.

Backup retention times can range from a few weeks to several months, and from the data protection standpoint this could be a critical issue.

In some cases, a backup copy can 'save your life' … and can protect the organisations against the risks related to a data breach event; if the breach is unlikely to result in a risk to the rights and freedoms of the natural persons whose personal data are referred to, the data controller doesn't need to notify the data breach to the relevant Supervisory Authority and to the data subjects (as per the cases n°1 and n°10 presented in the EDPB Guidelines n° 01/2021).

Backup is obviously just one of the several possible technical and organizational security measures that can be implemented to protect personal data and their processing; the possibility of a 'tailor-made' backup strategy makes it a versatile tool within the reach of every organization, even small and medium-sized ones.

Have a good backup!

Paola Limatola
DPO & Privacy Consultant
EADPP Italy Founding Member

Andrea Praitano
IT/OT Cybersecurity and Privacy Advisory Manager
EADPP Italy Founding Member

EADPP