Methods of data transfer

When collaborating with colleagues, we handle the sharing and transfer of data files on a daily basis. The options for the transfer of data depend on the scope of the transferred data.

1. Sending data as an e-mail attachment

Small-scale data (typically office application files, etc.) of several MBs are often transferred by e-mail (depending on the type of email client, files up to 10MB can be transferred in one message

What to watch out for...
Sending protected data by email is not recommended. However, it is essential to encrypt the files if this occurs. Emails are now commonly delivered to various mobile devices (phones, tablets, watches, etc.) with different levels of security, so the risk of disclosure is high when transferring unencrypted files.

2. Use of flash disks and USB drives

Today, very cheap flash or USB drives are used to transfer often relatively large amounts of data. Hence, when using encryption, there can be no objection to the use of this method, provided that the administration of end PCs allows them to be connected (many companies prohibit the use of USB ports for this purpose in order to protect data from being stolen). However, one must always pay attention to the secure transmission of the encryption key and realize that this method of transmission does not allow for verification of the data recipient.

What to watch out for...
As mentioned above, when using these portable media, it is essential to ensure the encryption of the stored data for security reasons. One must keep in mind the high risk of easily losing the media, i.e. the loss of stored data or their possible misuse.

3. Use of storage for one-time or time-restricted transfer of data

There are a number of web portals that allow you to conveniently upload even large amounts of data in order to provide them to or download them to other people (the identity of the persons authorized to download is determined by entering an e-mail address). These portals should also be seen as temporary data repositories, and one should keep in mind the above-mentioned aspects of the specific services.

a) CESNET “FileSender” service operated by CESNET z.s.p.o.

his service can be considered trusted and reliable for the reasons stated in paragraph 4.a) of the Section Categorization of storage, and so can be recommended for a one-time transfer of data. The service currently allows the transfer of data up to 1.9 TB per transfer (without HTML5 the limit is 2 GB per file) and now offers the option of encryption when uploading. The user is thus assured that the data stored on the portal is encrypted (the data is not readable even by the storage administrator). The user must then send the encryption password to the recipients (e.g., by e-mail, SMS, etc.).

b) Services of other commercial portals “ulož.to, uschovna.cz, e-disk, etc.”

On the other hand, these services are not recommend at all due to the high risk of data misuse.

4. Use of the “sharing” data storage functionality

The method of sharing within the appropriately selected data storage is certainly a good solution, as it permanently provides users authorized by you with access to the current shared data. Always be mindful of the sharing rights you provide to other users.

What to watch out for...
For sensitive or confidential scientific data, the choice of a suitable data storage method is essential, especially from the point of view of guaranteeing the security/confidentiality of stored data or the data management policy (see section 4.3).

5. Sharing within cloud storage

Cloud storage spaces have sophisticated data sharing capabilities for both cloud users and guests, allowing documents to be accessed with a time embargo or requiring user authentication for each access.

What to watch out for...
It is recommended to share within working groups (MS Teams).Considering the fact that several environments (so called tenants) are operated within the M365 services at the CU, be careful who you share your data with and whether

the user you have selected actually uses an identity in the tenant. Limit sharing via links for guests outside the tenant, as unauthorized users may also gain access to such data.