DEON On-Prem security

A DEON On-Prem Server runs inside the customer's corporate network and is installed by the internal IT.
The security and safety is under internal control.

- Any communication between the DEON Server and the DEON Clients is always encrypted with TLS. The highest available TLS level is negotiated between Client and Server based on the most current software version available. The encryption level can be adjusted by the customer.
- Customer-specific storage and encryption of user data and MS-SQL-DB (e.g TDE, Bitlocker, Vormetric, etc.)
- The customer can define which connections are allowed to the On-Prem DEON Server based on individual filters and firewall settings.
- The customer can define whether access is allowed only within the corporate network or enable external access over internet or VPN.
- User files can be saved either on the DEON Server or reside at their original source location (Local storage, Network folder, SharePoint, OneDrive, etc.) and only be linked into the DEON Workspace. By default the user can decide between both options. One option can also be forced according to the customer's preferences in the DEON Server Administration Settings.
- User data (Called Projects or Workspaces) in DEON are by default private and only accessible to the user who created them (Owner or Admin). Other DEON users have no access to other private Projects.
- To allow other users to see or edit a Project, the owner (Admin) of a Project can grant or withdraw other user's view rights or edit rights at any time.
- By design DEON automatically respects rights of integrated data sources. If a Project contains linked files (e.g. on network shares, OneDrive, SharePoint), those files will only be visible to users who also have the corresponding rights for the original storage location. Otherwise the file will be displayed as a grey box with a notification message inside the DEON Workspace.