

Compliance with the General Data Protection Regulation

Siemens respects the principles of data protection, in particular the data minimization requirements (privacy by design).

For the SINAMICS Startdrive product, this means that the product does not send any personal data to SIEMENS AG, unless the user explicitly requests it.

- a) If the SINAMICS Startdrive program comes to an unexpected end, the user has the opportunity to send diagnostics information to SIEMENS AG for analysis. If the user uses this option, the email address will also be collected, transmitted and saved in order to contact them in the event of queries.
- b) The Totally Integrated Automation UPDATER enables the user to check whether updates are available for SINAMICS Startdrive and to install them. The user can initiate this manually or enable the relevant setting for automatic updating. If the TIA Automation Update Server is used for checking or installation purposes, the IP address of the device used will be transmitted for technical reasons.

Furthermore, SINAMICS Startdrive only saves personal data in the project. The user is therefore responsible for ensuring compliance with the statutory data protection provisions. This applies in particular to the transfer of projects.

The following describes what data needs to be taken into account.

In the standard configuration, SINAMICS Startdrive saves the login details of the Windows user together with technical function data (e.g. time stamp) in the project, thus making personal references possible. This applies to the project as well as to all elements contained in it (e.g. devices and traces), and is designed to make it easier for the user to trace changes in large configurations.

This data can be viewed in the properties of the project and the elements in SINAMICS Startdrive ("Author" property) and, with the exception of the most recent change to the project, can be subsequently modified.

By generating the logins for the Windows users, personal data can be pseudonymized, for example by assigning a completely random login. However, this is done at the expense of the above-mentioned traceability of changes.

The SINAMICS Startdrive product only processes and saves additional personal data when the user explicitly enables one of the following functions.

- a) For user administration (security settings), the usernames created by the user are saved in order to be able to verify them during subsequent authentication.
- b) For multi-user engineering, various technical function data (e.g. time stamp) are saved together with the login details of the Windows user concerned in order to be able to trace project changes.

Please observe the relevant chapters in the SINAMICS Startdrive information system with regard to details of the specified functions.

By generating the login or username, personal data can be pseudonymized for both functions.

Deleting the project will cause all personal data saved within it to be deleted too. However, the particularities of multi-user engineering should be taken into consideration here, in particular the fact that the project not only needs to be deleted locally from the user's PC, but also from the server used.