AUVESY's position concerning its versiondog software and the requirements of the European GDPR

The GDPR data protection requirements and versiondog

The storage and use of personal data is subject to new regulations in the European Union as of 25 May 2018 with the coming into force of the General Data Protection Regulation (GDPR). In Germany, the existing Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) has been harmonised with the new GDPR; the revised version comes into force on the same date. The responsibility for the storage and use of personal data continues to be regulated by the German BDSG. Each company is itself responsible for the how it handles this data. It is important to AUVESY GmbH to provide its customers with information relevant to the GDPR of 25 May 2018 in the context of the versiondog data management system.

Storage of personal data in versiondog

The data management system versiondog stores both project data and the personal data of users who work on them. Data is stored by customers on their versiondog systems and not by AUVESY GmbH. The purpose of doing this is to enable customers to precisely track the changes that they make to their projects. Personal data is stored to keep a record of which users made which changes to which projects and why.

versiondog stores this data exclusively and explicitly to aid customers in their quality assurance and to speed up recovery from stoppages, particularly in automated environments. The requirements of the GDPR are met because the items of personal data that need to be stored are limited to the minimum necessary to fulfil the aforementioned purposes.

Customers can decide for themselves exactly what personal data is stored. Data input in versiondog only includes input fields that are necessary and relevant for a data management system. Furthermore, an anonymised user ID can be used to satisfy any additional data protection requirements. The versiondog software does not contain any input fields that request further personal data in categories such as ethnicity, religion or health.

The period for which personal data may be stored is limited in Chapter II, Article 5 of the GDPR to the period of time required for it to serve its purposes. The GDPR does not specify a precise period. In the case of a data management system, the time required for the retention of personal data to serve its purposes varies according to where and why the system is deployed. For example, food production in the USA and

for the US market must fulfil the requirements of the Food and Drug Administration (FDA), hence data must be stored for a comparatively long period of time in order to provide long-term verifiability that all FDA rules were adhered to. A similar situation exists in the automotive industry with regard to the manufacture of safety-related components.

Data collection and processing

The versiondog software qualifies as privacy-friendly according to the criteria set by the GDPR. Chapter IV, Article 25 defines these as "Privacy by Design" and "Privacy by Default". The versiondog data management system satisfies them both to the greatest possible extent. With regard to "Privacy by Design", versiondog limits the amount of personal user data that it requests to the minimum necessary. Furthermore, the versiondog system administrator can decide whether a name or an anonymised user number is appended to a Check-In. The administrator can alter this setting individually for any user at any time. Additionally, there is only one mandatory user details field; in line with the criterion "Privacy by Default", this field does not require a user's real full name. Any username or pseudonym can be entered. The administrator is also able to anonymise logged user data retrospectively. Thus versiondog administrators have the technical means to ensure that personal data is handled as required by Chapter IV, Article 25 of the GDPR.

Protection of personal data against misuse

The purpose of the versiondog data management software program is to store data. It does so in the form of versions, which are committed to the system database by the user. versiondog stores data centrally on Check-In, from where it is available to other users to Check-Out. As such, the latest approved version can always be obtained from the system. The Check-In of a version of a project can be deemed to be the point of approval and release. In this way, it will be clear which user made changes before a release and what those changes were. From the viewpoint of confidentiality and the protection of personal data against misuse, the versiondog software was designed to ensure the following:

- When a version is created, only the time and date when the data was stored is recorded. The length of time the user spent working on the project is neither visible nor recorded. The only thing that is visible is the fact that there is a new version available. It is not possible, either manually or automatically, to deduce from the change history or the data storage

- versiondog does not evaluate the quality of changes when versions are created. Differences are only detected for the purposes of storing and safeguarding data.

- Users are free to decide whether or not they store intermediate versions with unfinished changes. There is no requirement to create a version at any specific point in time and no requirement to create versions at a specific frequency. There are no versiondog settings that can be used to do this. The user decides when to create a version.

- The changes that are to be made before the creation of a new version of a project are decided upon by the versiondog user. The user is also responsible for documenting the changes. versiondog shows that changes have been made, but does not appraise or evaluate them in any way.

Because versiondog stores data for the purpose of change management, the question might arise as to whether or not the personal data gathered is also used as a means of employee surveillance. In view of the foregoing explication of data protection within the software, AUVESY's clear and unequivocal answer to this question is that it is not.

Access to and erasure of personal data in versiondog in accordance with the GDPR
One of the fundamental changes brought about by the new data protection regulation is the right to erasure ('right to be forgotten'). Chapter III, Article 17 of the GDPR states that "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay . . . ". And Chapter III, Article 15 of the GDPR states that "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data . . . ". Any response to such an enquiry must include details about how the data is stored as well as the type and extent of the processing that it is subject to. A legitimate request from the person for their data to be deleted must be complied with. The facility to meet the obligation to comply with a legitimate request to delete personal data in

accordance with Chapter III, Article 17 of the GDPR already exists in the versiondog software. There are two ways for a company's versiondog administrator to do this: one is to irretrievably delete the personal data from the entire system and the other is to anonymise the user data.

Future orientation of AUVESY GmbH

We are keenly aware of the trust that our customers place in our product versiondog and we sincerely thank them for it. In this context, it is of utmost importance to us to provide the best possible level of value and support. We achieve this by remaining at the cutting-edge of technical development, by responding to industry-specific requirements, and, of course, by complying with all relevant legal regulations. With this statement, AUVESY declares itself and its versiondog data management system well prepared for the European GDPR of 25 May 2018. Any future changes with implications for our products will be fully taken into account during their design and development.

Please do not hesitate to contact us if you have any questions to which you cannot find the answers here, or if your company has any individual requirements arising from the GDPR. We will be delighted to work together with you to find a solution that perfectly fits your situation.

Author:	Co-author:	Approved by:
Dr. Thorsten Sögding	**Georg Seiss M.A.**	**Dr. Tim Weckerle**
Director Customer Services	Business Development	CEO
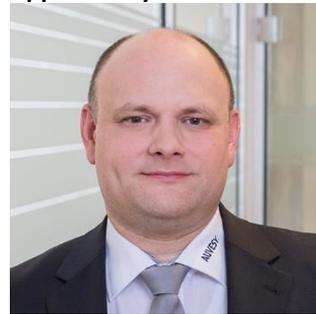
Landau, den 28.04.2018

Our Data Protection Officer will be pleased to answer any queries:

AUVESY.
Data Protection

Kay Tokner
Data Protection Officer
Tel: +49 (0)6341 – 6810 – 302
E-mail: Kay.Tokner@auvesy.de
AUVESY GmbH
Fichtenstrasse 38 B
D-76829 Landau, Germany
www.auvesy.com