SecDoc – GDPR-Compliant Documentation at the University of Münster

Thorsten Küfer[1], Dustin Gawron[2]

[1]University of Münster, Germany, thorsten.kuefer@uni-muenster.de
[2]University of Münster, Germany, dustin.gawron@uni-muenster.de

Keywords
GDPR, documentation, ISO 27000, data processing activities, web application

1. ABSTRACT

SecDoc is a web-based application for GDPR-compliant processing activity documentation which focuses on easy setup and usage. It has been developed at the University of Münster and is in use there. The goal is joint development and use by multiple universities. Future use should specifically address the IT security perspective of the technical and organisational measures in accordance with common standards (ISO 27000 (International Organization for Standardization, 2019), IT Grundschutz (Federal Office for Information Security (BSI))).

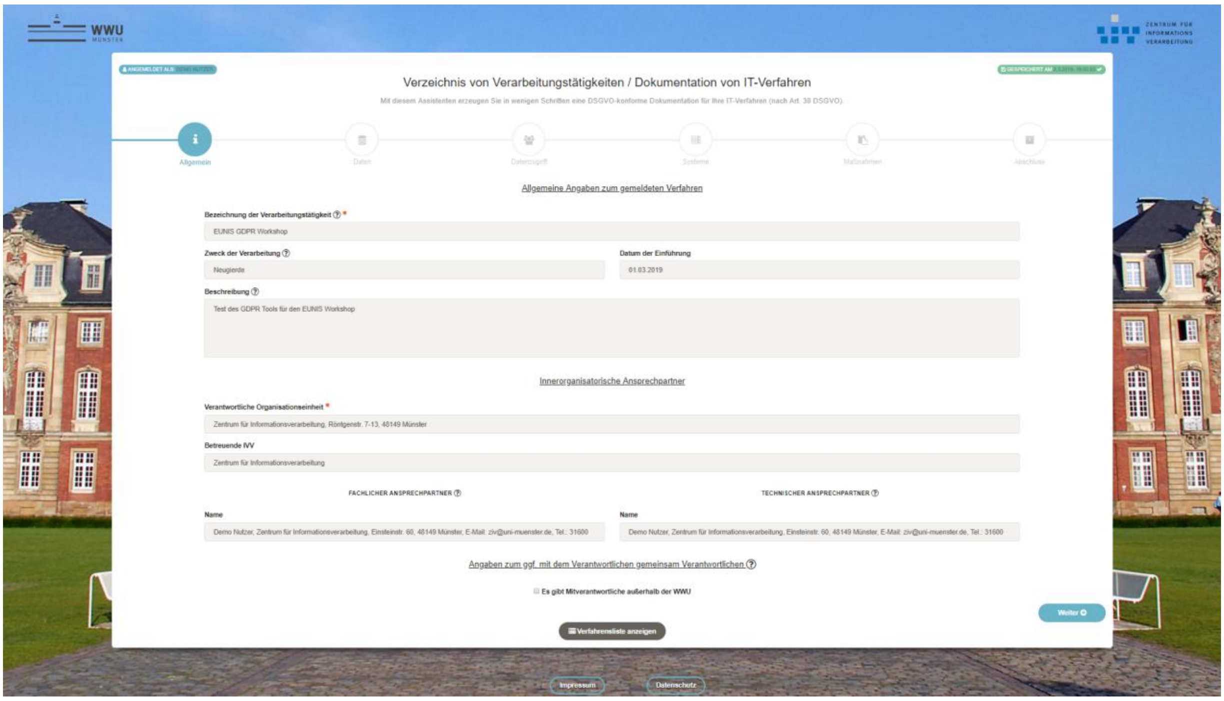
2. INTRODUCTION

The European Data Protection Regulation (GDPR), which was approved by the EU Parliament on 14 April 2016 and became effective on 25 May 2018, intends to improve data security and protect the privacy of individuals more effectively. For companies, organizations, and every other instance working with personal data this means greater responsibility and significantly increased effort. This paper focuses on one aspect in particular: the need for extended documentations of data processing activities. Article 30 GDPR states that “each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility” (European Parliament, 2016) and demands a description which and how personal information is processed. Usually there are many services working with personal data within an organisation and often those processes interact in between as well, exchanging data or sharing them with others. In most cases only the maintainer of such a service can understand and describe its processes. Consequently, no central authority can document all processes itself, but everyone in the organisation needs to partake and document their responsibilities. This calls for an easy to use and collaborative solution that particularly addresses the peculiarities of higher education institutions: SecDoc.

3. EXISTING SOLUTIONS

Textual templates are an easy solution for documenting single processes as they simply query all relevant aspects. They are available in form of Word or PDF files from various sources like ZENDAS (Data protection commissioner for Universities of Baden-Württemberg) (ZENDAS, 2018) or LDI NRW (Data protection commissioner of North Rhine-Westphalia) (Landesbeauftragte für Datenschutz und Informationsfreiheit NRW). However, such templates have many disadvantages in scenarios that are more complex. First, if users need to document several processes, it becomes a hassle to manage the respective files. Second, collaborative work on documents is difficult because a constant exchange of updated files is necessary to avoid parallel versions. Third, the templates do not enforce a standardized way of completion, making it necessary to discuss and decide on a joint approach in advance. Fourth, subsequent changes to the document can be a problem. In the worst case, the entire form must be filled out again, depending on the type of template. Fifth, there is no easy way to reference existing resources causing a lot of overhead and duplicate entries. In sum, these aspects make textual templates unsuitable for a larger environment in which various users work together to complete a documentation.

Tools for managing information security are another option and by now, many provide add-ons for GDPR compliant documentation, like verinice (SerNet, 2018). These systems have the major advantage of being able to document and reference most important details about the whole structure of available devices, users and services. If an Information Security Management System (ISMS) (International Organization for Standardization, 2019) is already in use and well documented, it is also suitable as basis for GDPR-compliant documentation. If not, however, the effort involved in introducing it cannot be justified by this purpose alone. Importing existing information can already be difficult and time-consuming. Furthermore, these applications do not focus on GDPR compliant documentation but offer a significantly larger range of functions. Consequently, the handling is clearly more difficult than necessary for the intended purpose – especially without previous training. Another drawback are limitations of collaborative work some systems impose, either by restricted licensing or by additional software requirements.



Verzeichnis von Verarbeitungstätigkeiten / Dokumentation von IT-Verfahren

Mit diesem Assistenten erzeugen Sie in wenigen Schritten eine DSGVO-konforme Dokumentation für Ihre IT-Verfahren (nach Art. 30 DSGVO)

Allgemeine Angaben zum gemeldeten Verfahren

Bezeichnung der Verarbeitungstätigkeit * : EUNIS GDPR Workshop

Zweck der Verarbeitung: Neugierde

Datum der Einführung: 01.03.2019

Beschreibung: Test des GDPR Tools für den EUNIS Workshop

Innerorganisatorische Ansprechpartner

Verantwortliche Organisationseinheit * : Zentrum für Informationsverarbeitung, Röntgenstr. 7-13, 48149 Münster

Betreuende IVV: Zentrum für Informationsverarbeitung

FACHLICHER ANSPRECHPARTNER

Name: Demo Nutzer, Zentrum für Informationsverarbeitung, Einsteinstr. 60, 48149 Münster, E-Mail: ziv@uni-muenster.de, Tel.: 31600

TECHNISCHER ANSPRECHPARTNER

Name: Demo Nutzer, Zentrum für Informationsverarbeitung, Einsteinstr. 60, 48149 Münster, E-Mail: ziv@uni-muenster.de, Tel.: 31600

Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen

□ Es gibt Mitverantwortliche außerhalb der WWU

Figure 1 - SecDoc Main View

4. SECDOC

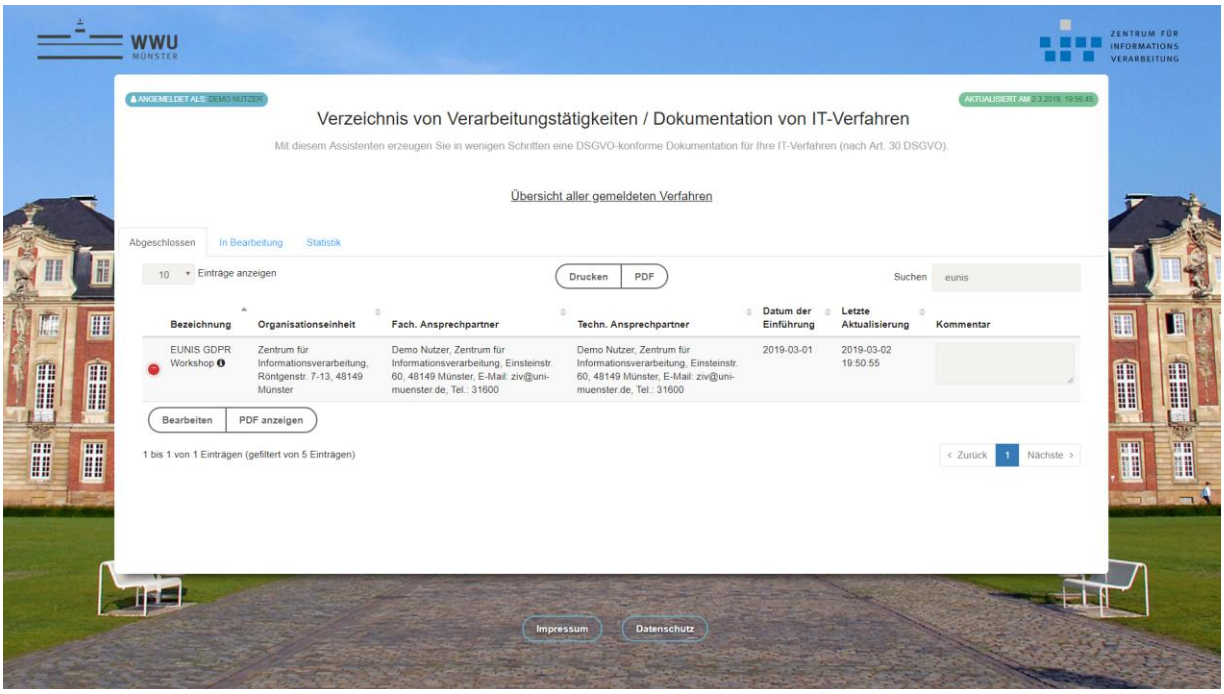
SecDoc (Westfälische Wilhelms-University, 2019) was born from the idea of developing an easy to use tool for GDPR compliant documentations that addresses the organisational specifics of a university. It should not require any significant additional setup or overhead. The solution is a light-weight web application that can be accessed simply with an HTML 5 compliant browser, eliminating the need for additional software.

The application consists of an interactive form originally based on the ZENDAS template (ZENDAS, 2018) which was adapted and extended in cooperation with our data protection officers (DPOs).

SecDoc guides users through the entire documentation process in six steps: 1) general information about processing activity, including contact information, 2) data categories, 3) data access, 4) relevant IT systems, 5) technical and organisational measures (security of processing), 6) settings and finish. To help users fill out the form and further harmonise the structure of different documentations, hints and suggestions (e.g. for contact information, organisational units, computer systems) are offered during completion. The current progress is saved automatically on a backend server once a step is completed. Manual saving is also possible. This enables users to continue their work where they left off. Once a documentation is completed, a compact PDF version is generated and any person declared as responsible contact person of the process is notified by email.

By default, only the creator, organisational and technical contact persons as well as the DPOs can access a documentation. These persons can grant role based access and editing rights to other users, thereby eliminating the need to send documents back and forth for collaboration. DPOs have access to all available documentations, whether they are still in progress or completed, enabling them to assist users in filling out the form and to keep track of possible issues.

The frontend is a mix of HTML and JavaScript to enable interactivity. It uses Bootstrap for a responsive web design. The backend is a light-weight PHP script, handling Ajax requests from the frontend. It uses a standalone SQLite database, which can be easily replaced by other database systems in case higher performance is needed. All information entered by users is processed in JSON format, which makes it easy to access the data with third-party or future tools (e.g. verinice). The PDF generation is performed on the server using MPDF. The backend uses existing services where applicable. The login, for example, is handled with our university's SSO solution, while user information, role information, and information about existing computer systems is retrieved from our central databases.



WWU
MÜNSTER
ZENTRUM FÜR INFORMATIONSVERARBEITUNG
ANGEMELDET ALS: DEMO NUTZER
AKTUALISIERT AM 2.3.2019, 19:56:45

Verzeichnis von Verarbeitungstätigkeiten / Dokumentation von IT-Verfahren

Mit diesem Assistenten erzeugen Sie in wenigen Schritten eine DSGVO-konforme Dokumentation für Ihre IT-Verfahren (nach Art. 30 DSGVO).

Übersicht aller gemeldeten Verfahren

Abgeschlossen
In Bearbeitung
Statistik
10 Einträge anzeigen
Drucken
PDF
Suchen
eunis

Bezeichnung	Organisationseinheit	Fach. Ansprechpartner	Techn. Ansprechpartner	Datum der Einführung	Letzte Aktualisierung	Kommentar
EUNIS GDPR Workshop	Zentrum für Informationsverarbeitung, Röntgenstr. 7-13, 48149 Münster	Demo Nutzer, Zentrum für Informationsverarbeitung, Einsteinstr. 60, 48149 Münster, E-Mail: ziv@uni-muenster.de, Tel.: 31600	Demo Nutzer, Zentrum für Informationsverarbeitung, Einsteinstr. 60, 48149 Münster, E-Mail: ziv@uni-muenster.de, Tel.: 31600	2019-03-01	2019-03-02 19:50:55	

1 bis 1 von 1 Einträgen (gefiltert von 5 Einträgen)

Figure 2 - DPO View

5. FUTURE PLANS

Even though the application is already in use, there are still many aspects we would like to cover in the future. First, we want to further simplify usage by creating and providing templates for commonly used services such as email, file service, ticket system or Active Directory systems. This enables users to copy templates within SecDoc and they only need to adjust the content according to their individual setup. Secondly, we want to extend the application to include a good and easy to use solution for documenting technical and organizational measures (TOMs) (as required by Art. 32 GDPR) (European Parliament, 2016) as well as a method for carrying out data protection impact assessments (as required by Art. 35 GDPR) (European Parliament, 2016). Thirdly, we want to find a suitable solution to support multiple languages, as the application is only available in German at the moment. In the end the DPO view of all processing activities could be implemented with a dashboard showing various statistics and information helping the DPO's tasks.

In addition to these development goals, there are also organizational aspects that need clarification. A data protection management system (DPMS) should be established before the introduction of the documentation tool. Official regulations and guidelines need to be created at Münster of University to enforce the use of SecDoc in the long run. The DPMS should address the responsibilities for documentation and set up decentral contact persons. In order to further establish SecDoc for the documentation of processing activities at the University of Münster, we need user-friendly manuals and training for decentral DPOs who can support the users directly and efficiently. Currently, the most difficult part is to decide on the necessary granularity of documentations.

Various German universities have expressed their interest in SecDoc and cooperation for further development. Joint working groups have already been formed to promote the application and collect feedback for new features. Specifically it has been presented at the EUNIS GDPR and Information Security workshop held at Brunel University London (Information Security Special Interest Group, 2018). The code is published under the AGPLv3 license (Westfälische Wilhelms-University, 2019) and everyone is invited to test SecDoc, give constructive feedback and support further development.

6. REFERENCES

European Parliament, C. o. (2016, 04 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Retrieved from EUR-Lex - 32016R0679 - EN - EUR-Lex: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Federal Office for Information Security (BSI). (n.d.). *IT-Grundschutz*. Retrieved from https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

Information Security Special Interest Group. (2018, 12 10). *EUNIS GDPR and Information Security workshop*. Retrieved from http://www.eunis.org/gdpr-workshop-london/

International Organization for Standardization. (2019, 03 01). *ISO/IEC 27000 family - Information security management systems*. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

Landesbeauftragte für Datenschutz und Informationsfreiheit NRW. (kein Datum). *Das neue Verarbeitungsverzeichnis nach Artikel 30 DS-GVO*. Von https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Betriebliche_Datenschutzbeauftragte/Inhalt/Das-neue-Verarbeitungsverzeichnis-nach-Artikel-30-DS-GVO/Das-neue-Verarbeitungsverzeichnis-nach-Artikel-30-DS-GVO.html abgerufen

SerNet. (2018, 4 20). *verinice 1.16 helps you to handle the GDPR*. Retrieved from https://verinice.com/en/news/detail/mit-verinice-116-die-eu-dsgvo-im-griff/

Westfälische Wilhelms-University. (2019). *SecDoc Demo*. Von https://www.uni-muenster.de/ZIVtest/secdoc-demo/ abgerufen

Westfälische Wilhelms-University. (2019). *ZIV GitLab*. Von https://zivgitlab.uni-muenster.de/wwu-cert/secdoc/ abgerufen

ZENDAS. (19. 01 2018). *ZENDAS Verzeichnis von Verarbeitungstätigkeiten (VVT) [de]*. Von ZENDAS Verzeichnis von Verarbeitungstätigkeiten (VVT) (Datenschutz in der Hochschule) [Restricted access]: https://www.zendas.de/service/VVT.html abgerufen

7. AUTHORS' BIOGRAPHIES

Thorsten Küfer is information security officer at the IT center of the University of Münster, Germany. He graduated at Münster University in 2004 and holds a diploma in mathematics and computer science. He coordinates the university's information security management team (IV-S) and the computer emergency response team (WWU-CERT). IV-S is the steering committee for organizational aspects of information security.

Dustin Gawron is a graduate student of the master degree course in computer science at the University of Münster, Germany. In 2017 he received his bachelor's degree in computer science from the same institution. Currently he is working as a student assistant for the information security management team (IV-S) at the IT center of Münster University.