

Datenschutzerklärung gem. Art. 13 DSGVO

Projekt/Anlass: Betrieb eines zentralen Log-Servers und SIEM-Systems

Stand: 2022-12-15 16:36:25

1. Name und Anschrift der verantwortlichen Stelle

Die verantwortliche Stelle im Sinne der EU-Datenschutzgrundverordnung (DSGVO) und anderer nationaler Datenschutzgesetze der Mitgliedsstaaten sowie sonstiger datenschutzrechtlicher Bestimmungen ist die:

Westfälische Wilhelms-Universität Münster,
vertreten durch den Rektor Prof. Dr. Johannes Wessels,
Schlossplatz 2, 48149 Münster
Tel.: +49 251 83-0
E-Mail: verwaltung@uni-muenster.de

Bei inhaltlichen Rückfragen zum Projekt wenden Sie sich bitte direkt an die fachliche Ansprechperson:

Dustin Gawron, Mitarbeiter*innen der WWU IT, Tel.: +49 251 83 31534, E-Mail: d.gawron@uni-muenster.de

WWU IT, Röntgenstr. 7-13, 48149 Münster

2. Kontaktdaten der/des Datenschutzbeauftragten

Die/den Datenschutzbeauftragte*n der verantwortlichen Stelle erreichen Sie unter:

Stabsstelle Datenschutz
Schlossplatz 2, 48149 Münster
Tel.: + 49 251 83-22446
E-Mail: datenschutz@uni-muenster.de

3. Datenverarbeitung im Rahmen des Projektes "Betrieb eines zentralen Log-Servers und SIEM-Systems"

Beschreibung des Projekts:

Das WWU-CERT betreibt ein Security Information and Event Management System (SIEM) und erhält die dafür benötigten Daten aus der WWU IT und den IVVen. Sicherheitsrelevante Informationen (z. B. Logs) werden im zentralen SIEM zusammengeführt und durch das WWU-CERT auf Auffälligkeiten

hinsichtlich der IT-Sicherheit analysiert. So entsteht eine zentrale Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse. In den Richtlinien "RL14 Protokollierung und zentrales Logging" und "RL15 Detektion und Behandlung von Sicherheitsvorfällen" werden Ziele, Maßnahmen, Umsetzung, Rechtsgrundlage sowie der Zweck der benötigten Log-Informationen spezifiziert. Zugriff auf alle Daten im SIEM haben ausschließlich Mitarbeiter des WWU-CERT. Die ursprünglichen Log-Daten werden bis zu 30 Tage gespeichert, die daraus gewonnenen Events bzw. Auffälligkeiten bis zu einem Jahr. Eine Verwendung dieser Daten für Zwecke der Leistungs- und/oder Verhaltenskontrolle der Beschäftigten ist unzulässig.

a) Umfang der Datenverarbeitung

Im Rahmen des Projekts "Betrieb eines zentralen Log-Servers und SIEM-Systems" verarbeiten wir von Ihnen folgende Daten:

1. Einwahl-Verbindungsdaten (Startzeit, Stopzeit, IP-Adresse, Kennung)
2. Endgerätedaten (IP-Adresse, MAC-Adressen, Netbios-Name, Zeitpunkt)
3. Antivirusdaten (Nutzer, Endgerät, Pfad, Dateiname, Schadsoftware, Zeitpunkt)
4. Windows An- und Abmeldedaten der aus dem Internet erreichbaren RDP-Server (Kennung, IP-Adresse, Zeitpunkt)
5. E-Mail-Daten (Sender, Empfänger, Betreff (zu prüfen), einliefernde IP-Adresse, Zeitpunkt)
6. System Log-Daten (Nutzer, Systembefehl, Zeitpunkt)
7. DNS-Daten (Angefragter DNS-Name, anfragende IP-Adresse, Zeitpunkt)
8. Netflow-Daten (Quell-IP, -Port, Ziel-IP,-Port, Zeitpunkt, Bytes)

b) Zwecke der Datenverarbeitung

Erkennung von Angriffen, kompromittierten Systemen und Nutzerkennungen

c) Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Die folgenden Rechtsgrundlagen laut DSGVO liegen der Verarbeitung Ihrer Daten zu Grunde:

Rechtsgrundlage laut DSGVO	Erläuterungen
Art. 6 (1) c) - Rechtliche Verpflichtung	§ 12 TTDSG, § 3 Abs. 1 DSGVO NRW i.V.m. §10 u. §13, Nutzungsordnung des ZIV und der IVVen §7 Abs. 6
Art. 6 (1) f) - Berechtigte Interessen	Erwägungsgrund 49, Netz- und Informationssicherheit als überwiegendes berechtigtes Interesse

d) Weitere Empfänger*innen Ihrer personenbezogenen Daten

Ihre oben genannten personenbezogenen Daten, werden an folgende Empfänger*innen innerhalb bzw. außerhalb der Institution weitergegeben:

Interne Empfänger*innen:

Interne Stelle oder Personen	Zweck bzw. Tätigkeit
WWU-CERT	Erkennung, Aufklärung und Behebung von Sicherheitsvorfällen.
Administratoren	Einsicht in eingelieferte Daten zur Störungsbehebung (gleicher Umfang wie auf den Ursprungssystem).

Externe Empfänger*innen:

Keine externen Empfänger

e) Dauer der Speicherung der personenbezogenen Daten

Ihre oben genannten personenbezogenen Daten werden so lange gespeichert, wie sie für die oben genannten Zwecke benötigt werden. Falls im Rahmen des in der konkreten Datenschutzerklärung jeweils beschriebenen IT-Systems bzw. Projekts die Verarbeitung der personenbezogenen Daten auf Ihrer Einwilligung beruht, werden die Daten gelöscht, wenn Sie Ihre Einwilligung widerrufen, es sei denn, es besteht eine andere Rechtsgrundlage für die weitere Speicherung.

Folgende Fristen für Anonymisierung oder Löschung der Daten wurden gesondert festgelegt:

Daten (siehe a))	Pseudonymisierungs- oder Löschfrist
1, 2, 3, 4, 5, 6, 7, 8	bis zu 30 Tage gesamte Log-Daten
1, 2, 3, 4, 5, 6, 7, 8	bis zu einem Jahr sicherheitsrelevante Meldungen

4. Ihre Rechte als betroffene Person

Sie haben ein Recht auf Auskunft über Ihre verarbeiteten personenbezogenen Daten (Art. 15 DSGVO), ein Recht auf Berichtigung Ihrer personenbezogenen Daten (Art. 16 DSGVO), ein Recht auf Löschung (Art. 17 DSGVO), ein Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) und ein Recht auf Widerruf Ihrer Einwilligung (Art. 7 Abs. 3 DSGVO).

Außerdem haben Sie das Recht, Beschwerde bei einer Aufsichtsbehörde einzulegen, z. B. bei der folgenden Behörde:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Postfach 20 04 44, 40102 Düsseldorf

Tel.: +49 211 38424-0

E-Mail: poststelle@ldi.nrw.de