

Datenschutz

Prüfungsbericht

Notes2conf

<https://notes2conf.de/>

mip Consult GmbH

Wilhelm-Kabus-Str. 9

10829 Berlin



Inhalt

1	PRÜFUNGSGEGENSTAND	3
2	ZUSAMMENFASSUNG DER PRÜFUNGSERGEBNISSE.....	3
3	ERKENNTNISSE DER PRÜFUNG	3
4	EMPFEHLUNGEN	6
5	BESTÄTIGUNG.....	6

1 Prüfungsgegenstand

Die Dacher Systems GmbH, Seeburger Str 25c, 13581 Berlin (kurz: „DS“), hat die mip Consult GmbH, Wilhelm-Kabus-Straße 9, 10829 Berlin, Deutschland mit der Prüfung des Gateway-Tools „**Notes2conf**“ beauftragt. In der Zeit vom 01.12.2020 bis 20.01.2021 wurden auf Grundlage von Interviews mit DS-Mitarbeitern und auf Basis der technischen Dokumentation analysiert, inwieweit die aus der europäischen Datenschutzgrundverordnung (DSGVO) abzuleitenden Vorgaben an Software eingehalten werden.

Bei „Notes2conf“ handelt es sich um eine Applikation, die für Nutzer von HCL Notes eine einfache Integration von Video-Konferenz-Diensten ermöglicht.



2 Zusammenfassung der Prüfungsergebnisse

Aufgrund der bei der Prüfung gewonnenen Erkenntnisse ist festzustellen, dass „**Notes2conf**“ die Anforderungen der europäischen Datenschutzgrundverordnung (DSGVO) erfüllt. Die Umsetzung der in Kapitel 4 benannten Maßnahmen wird empfohlen.

3 Erkenntnisse der Prüfung

Im Rahmen der Untersuchung wurden folgende Punkte geprüft:

- **Datenminimierung, Art. 6 Abs. 1 lit c DSGVO**

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Die Daten, die auf dem Notes2conf Server verarbeitet und für den Zeitraum der Herstellung der Konferenz zwischengespeichert werden, sind die Daten der Einladungs-E-Mail des Organisators. Hierbei handelt es sich um folgende Daten:

- Subject (Besprechungsthema)
- Datum (der Besprechung)
- Uhrzeit (Beginn und Ende)
- E-Mail-Adresse des Organisators und ggf. Name als Meta-Information zur E-Mail-Adresse
- E-Mail-Adresse der Teilnehmer und ggf. Name als Meta-Information zur E-Mail-Adresse

Bei den verwendeten Daten handelt es sich im Wesentlichen um den Namen des Organisators und die Namen der Teilnehmer sowie deren E-Mail-Adressen. Diese Daten sind für die Initiierung einer Videokonferenz notwendig.

Anmelddaten zu den jeweiligen Videokonferenz-Anbietern werden nicht von Notes2conf verarbeitet.

Die Authentifizierung auf der Notes2conf Landingpage für den dort bereitgestellten Warteraum erfolgt über den Einladungslink zur Besprechung. Der Einladungslink (enthalten in der E-Mail an den jeweiligen Teilnehmer) wird durch eine entsprechend lange Kette per Zufallsgenerator ermittelter Zeichen generiert.

- **Speicherbegrenzung, Art. 5 Abs. 1 lit e DSGVO**

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“).

Nach Beendigung einer über Notes2conf initiierten Besprechung (sofern es sich nicht um eine wiederkehrende Besprechung handelt) löscht Notes2conf sämtliche Daten (d.h. bei Ereigniseintritt "Uhrzeit - Ende"). Bei wiederkehrenden Besprechungen werden die Daten gelöscht, sobald die Besprechung vom Organisator gelöscht wird, oder die letzte, wiederkehrende Besprechung beendet wurde.

- **Integrität und Vertraulichkeit, Art. 5 Abs. 1 lit f, Art. 32 DSGVO**

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Notes2conf wird auf Servern eines renommierten deutschen Anbieters in Deutschland gehostet. Über die Verarbeitung der dort erhobenen Daten wir in einer Datenschutzinformation gemäß Art. 13 DSGVO informiert. Die Notes2conf Webseite ist per HTTPS gesichert. Ferner unterstützen die Notes2conf Mail-Server die Verschlüsselung des Transportweges per TLS. Wenn der E-Mail-Server des Absenders ebenfalls den verschlüsselten Versand unterstützt, werden sämtliche E-Mails auf dem Transportkanal verschlüsselt und grundsätzlich ist dann keiner der Server-Knotenpunkte, über den die E-Mails im Internet laufen, in der Lage mitzulesen. Zugriff auf die E-Mail (und die Anhänge) haben in diesem Fall mithin nur die Serverbetreiber des Empfängers und des Absenders.

```

seconds test stage and result
[000.000] DNS LOOKUPS
[000.000] created RESOLVER
[000.253] NS 10.132.36.231
[000.253] MX (10) mail.dacher-systems.com
[000.545] A-->mail.dacher-systems.com 90.187.228.181

seconds test stage and result
[000.000] Trying TLS on mail.dacher-systems.com[90.187.228.181:25] (10)
[000.102] Server answered
[006.806] <--220-mailsec.dacher-systems.com ESMTP Proxmox
220 mailsec.dacher-systems.com ESMTP Proxmox
[006.806] We are allowed to connect
[006.806] -->EHLO www12-do.checktls.com
[006.910] <--250-mailsec.dacher-systems.com
250-PIPELINING
250-SIZE 30485760
250-VRFY
250-ETRN
250-STARTTLS
250-EHANCEDSTATUSCODES
250-8BITMIME
250-SMTPUTF8
250 CHUNKING
[006.910] We can use this server
[006.910] TLS is an option on this server
[006.910] -->STARTTLS
[007.014] <--220 2.0.0 Ready to start TLS
[007.014] STARTTLS command works on this server
[007.168] Connection converted to SSL
SSLVersion in use: TLSv1_3
Cipher in use: TLS_AES_256_GCM_SHA384
Perfect Forward Secrecy: yes
Certificate #1 of 1 (sent by MX):
Cert VALIDATION ERROR(S): self signed certificate
So email is encrypted but the recipient domain is not verified
Cert Hostname VERIFIED (mail.dacher-systems.com = *.dacher-systems.com)
Not Valid Before: Mar 1 09:42:53 2019 GMT
Not Valid After: Feb 26 09:42:53 2029 GMT
subject= /O=dacher-systems.com/OU=Proxmox Mail Gateway/CN=*.dacher-systems.com
issuer= /O=dacher-systems.com/OU=Proxmox Mail Gateway/CN=*.dacher-systems.com
[007.196] -->EHLO www12-do.checktls.com
[007.369] <--250-mailsec.dacher-systems.com
250-PIPELINING
250-SIZE 30485760
250-VRFY
250-ETRN
250-EHANCEDSTATUSCODES
250-8BITMIME
250-SMTPUTF8
250 CHUNKING
[007.370] TLS successfully started on this server
[007.370] -->MAIL FROM:<test@checktls.com>
[007.489] <--250 2.1.0 Ok
[007.489] Sender is OK
[007.489] -->QUIT
[007.589] <--221 2.0.0 Bye

```

Getestet via <https://www.checktls.com/TestReceiver>

Ein Prozess für das Patch-Management ist implementiert und stellt regelmäßige und rechtzeitige Software-Updates sicher, ggf. unter Verwendung von Patch-Management-Software.

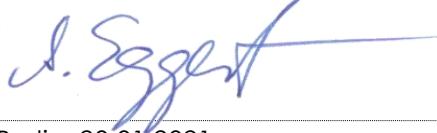
4 Empfehlungen

Es werden folgende Maßnahmen empfohlen:

- Einsatz eines Zertifikats einer kommerziellen Zertifizierungsstelle (CA) anstelle eines selbst generierten Zertifikats

5 Bestätigung

Der Auditor kommt nach Prüfung zu dem Ergebnis, dass Dacher Systems GmbH mit „**Notes2conf**“ die Vorgaben der DSGVO im Hinblick auf technisch-organisatorische Maßnahmen zur datenschutz-konformen Übertragung der durch „**Notes2conf**“ verarbeiteten personenbezogenen Daten erfüllt.

A handwritten blue ink signature of the name "Dr. Eggert".

Berlin, 20.01.2021

Rechtsanwalt
zertifizierter Datenschutzbeauftragter (TÜV)
zertifizierter Datenschutz-Auditor (TÜV)