

Beispiel Verzeichnis der Verarbeitungen durch den Verantwortlichen anhand der Verarbeitung „E-Mail-Dienst“

Angaben gemäß Art.30 Abs. 1 EU DS-GVO:

Name, Kontaktdaten Verantwortlicher

Hochschule Musterstadt, vertreten durch den Rektor Frank Mustermann, Musterstraße 1, 00000 Musterstadt

Name, Kontaktdaten des behördlichen Datenschutzbeauftragten

Der behördliche Datenschutzbeauftragte der Hochschule Musterstadt Max Mustermann, Musterstraße 1, 00000 Musterstadt, datenschutz@hochschule-musterstadt.de, +49 6666 007 215

Zwecke der Verarbeitung

Ermöglichung der Übermittlung und des Empfangs von nutzerdefinierten elektronischen Nachrichten per E-Mail

Kategorien Betroffener und Daten

Angehörige und Mitglieder der Hochschule Musterstadt als Absender und Empfänger

- **Bestandsdaten:** Sämtliche Kontoinformationen zum E-Mail-Konto wie z.B. Kontoname, Aliase, Gruppenzugehörigkeiten, etc.
- **Verkehrsdaten:** Zeitpunkt Abrufe oder Versand, Absender- und Empfängeradresse von Nachrichten, Datenvolumen, Anzahl Datenpakete...
- **Inhaltsdaten:** Nachrichteninhalte (Achtung: besonderer Schutz durch das Fernmeldegeheimnis, wenn die Privatnutzung nicht wirksam ausgeschlossen ist)

Absender, die Nachrichten an Angehörige und Mitglieder der Hochschule Musterstadt versenden:

- **Verkehrsdaten:** Zeitpunkt Abrufe oder Versand, Absender- und Empfängeradresse von Nachrichten, Datenvolumen, Anzahl Datenpakete...
- **Inhaltsdaten:** Nachrichteninhalte (Achtung: besonderer Schutz durch das Fernmeldegeheimnis, wenn die Privatnutzung nicht wirksam ausgeschlossen ist)

Kategorien Empfänger

Bestimmungsgemäße Empfänger von E-Mails, Nutzerverwaltung (Bestandsdaten), Administratoren

Ggf. Übermittlungen Drittland / Nennung

Eine Übermittlung in Drittländer erfolgt gegebenenfalls auf Veranlassung des Absenders einer Nachricht, indem er Nachrichten an Empfänger in Drittländern versendet. Bestands-, Verkehrs- und Inhaltsdaten werden durch die Hochschule Musterstadt nicht in Drittländer übermittelt.

Wenn möglich: Löschfristen

Bestandsdaten:

Mit Ablauf des auf die Beendigung folgenden Jahres (§ 95 Abs. 3 TKG)

Verkehrsdaten:

Grundsätzlich erfolgt die Löschung nach 7 Tagen (§ 100 Abs. 1 TKG + aktuelle Rechtsprechung des BGH zur Speicherung von Verkehrsdaten zur Störungserkennung). Wird ein Teilbestand zur Behebung einer konkreten Störung benötigt, so bleiben diese Daten bis zur Behebung der Störung gespeichert.

Inhaltsdaten:

Bei POP3 erfolgt keine dauerhafte Speicherung der Mails auf den Mailservern, sondern nur bis zum Abruf durch den Inhaber des Mailkontos. Bei IMAP liegt die Entscheidung über die Löschung in aller Regel primär beim Inhaber des Mailkontos. Besteht eine Löschpolicy bei Beendigung des Nutzungsverhältnisses, ist hier anzugeben, wie in diesen Fällen mit den Mails verfahren wird.

Wenn möglich: Allgemeine Beschreibung TOM

Allgemeine Beschreibung der ergriffenen Sicherheitsmaßnahmen:

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);