Eine Stunde Datenschutz

Sicherheit durch Technik - TOMs einfach erklärt

Eine Stunde Datenschutz

- Webinar-Reihe des Arbeitskreises Datenschutz sowie des Servicezentrums, Team Rechtsservice, der Wirtschaftskammer Kärnten

- Vortragende:

  Mag. Günther Zikulnig

  Ing. Hannes Strasser

  Ing. Walter Wratschko

- Moderation:

  Dr. Christina Kitz-Überall

Eine Stunde Datenschutz

Sicherheit durch Technik – TOMs einfach erklärt

- DDSB.AT Beratung GmbH **T** +43 (0) 1 42 000 5050 I **E** guenther.zikulnig@ddsb.at **I** www.ddsb.at I Sorgogasse 10/32, 1130 Wien
  Zikulnig Consulting **T** +43 (0) 664 / 819 33 35 I **E** office@zikulnig.at **I** www.zikulnig.at
  Klagenfurter Straße 9, A-9100 Völkermarkt

- IHS e.U. Consulting & Coaching **T** +436641393935 I **E** strasser@ihs-beratung.at I https://www.ihs-beratung.at/ I Mozartstraße 56, Tür 20,9020 Klagenfurt am Wörthersee

- Ing. Walter Wratschko I Office Klagenfurt: Brunnplatz 5, 9020 Klagenfurt, Office Wien: Esteplatz 3, 1030 Wien I T +43 699 1504 3860 I
  E walter.wratschko@datenschutz-sued.at www.datenschutz-sued.at

- https://www.wko.at/branchen/k/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/arbeitskreis-datenschutzexperten.html

- Dr. Christina Kitz-Überall, Servicezentrum, Rechtsservice, Wirtschaftskammer Kärnten
  E christina.kitz-ueberall@wkk.or.at I **T** 05 90 90 4 - 723

Ein Stunde Datenschutz

Sicherheit durch Technik - TOMs einfach erklärt

UNiQUARE Software Development GmbH

Mag. Günther Zikulnig
Ing. Hannes Strasser

DDSB.AT
DATENSCHUTZ & DIGITALISIERUNG

IHS Consulting & Coaching

Sicherheit durch Technik - TOMs einfach erklärt

1. Grundlagen
2. Begriffsbestimmungen
3. Aufbau und Dokumentation
4. Mitarbeiter
5. Fragen

1. TOMs - Grundlagen

Datenschutz=

a) Datenschutzrecht

rechtl. Voraussetzung (darf ich, warum…)

b) Datensicherheit

Schutz sicherstellen (wie, durch welche Maßnahmen…)

1. TOMs - Grundlagen

Worum geht`s eigentlich?

„Verantwortlicher und Auftragsverarbeiter“

„geeignete technische und organisatorische Maßnahmen“

„ein dem Risiko angemessenes Schutzniveau“

„zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten“

(Art. 32 DSGVO)

1. TOMs - Grundlagen

Technik vs. Organisation

Technik:
- Soft- und Hardwarelösungen
- Physische Maßnahmen

Organisation:
- definierte Abläufe/Prozesse
- Vereinbarungen (mit Mitarbeitern, Lieferanten, Partnern etc.)
- Schulungen
- Besucherregistrierung

1. TOMs - Grundlagen

Ähnlichkeit zu NIS2 Anforderungen

NIS2	DSGVO
Cybersicherheit	Schutz personenbezogener Daten
10 Risikomanagementmaßnahmen	technische und organisatorische Maßnahmen
Berichts- und Meldepflichten	Meldepflichten
Sanktionen	Sanktionen

2. TOMs - Begriffsbestimmung

- **Personenbezogene Daten**

  Daten, die sich auf eine identifizierte/-bare natürliche Person beziehen
- **Verantwortlicher**

  über die Zwecke und Mittel der Datenverarbeitung entscheidet
- **Auftragsverarbeitervertrag**

  Datenverarbeitung im Auftrag des Verantwortlichen
- **Data Breach**

  Verletzung des Schutzes personenbezogener Daten

2. TOMs - Begriffsbestimmung

- **Stand der Technik**

  „Entwicklungsstand…erprobt und bewiesen ist“

- **Privacy by design**

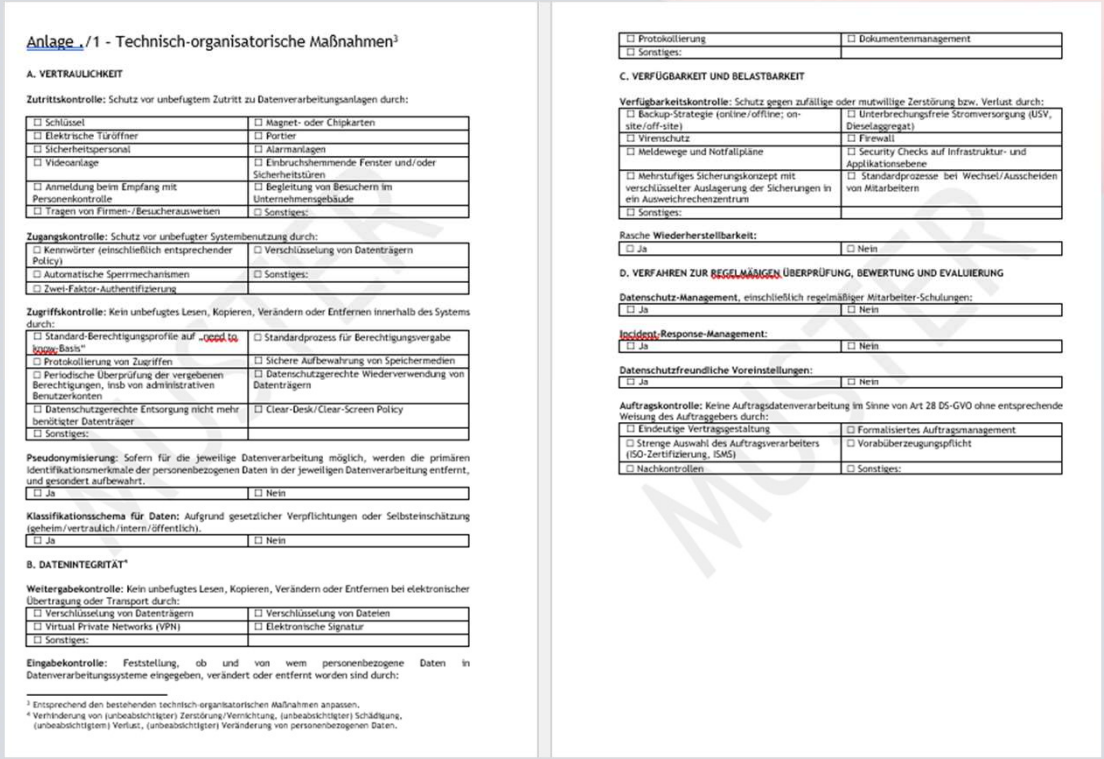
  Datenschutz durch Technikgestaltung (schon bei Entwicklung/ Programmierung Datenschutzvorgaben zu berücksichtigen)

- **Privacy by default**

  Datenschutz durch datenschutzfreundliche Voreinstellung („Datenschutz ab Werk“ – schon bei Auslieferung datenschutzfreundlich voreingestellt)

3. TOMs – Aufbau und Dokumentation

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit
- Wiederherstellbarkeit
- Dokumentation



Anlage ./1 - Technisch-organisatorische Maßnahmen[3]

A. VERTRAULICHKEIT

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☐ Schlüssel	☐ Magnet- oder Chipkarten
☐ Elektrische Türöffner	☐ Portier
☐ Sicherheitspersonal	☐ Alarmanlagen
☐ Videoanlage	☐ Einbruchshemmende Fenster und/oder Sicherheitstüren
☐ Anmeldung beim Empfang mit Personenkontrolle	☐ Begleitung von Besuchern im Unternehmensgebäude
☐ Tragen von Firmen-/Besucherausweisen	☐ Sonstiges:

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☐ Kennwörter (einschließlich entsprechender Policy)	☐ Verschlüsselung von Datenträgern
☐ Automatische Sperrmechanismen	☐ Sonstiges:
☐ Zwei-Faktor-Authentifizierung	

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☐ Standard-Berechtigungsprofile auf „need to know-Basis"	☐ Standardprozess für Berechtigungsvergabe
☐ Protokollierung von Zugriffen	☐ Sichere Aufbewahrung von Speichermedien
☐ Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten	☐ Datenschutzgerechte Wiederverwendung von Datenträgern
☐ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☐ Clear-Desk/Clear-Screen Policy
☐ Sonstiges:	

Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

☐ Ja	☐ Nein

Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☐ Ja	☐ Nein

B. DATENINTEGRITÄT[4]

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☐ Verschlüsselung von Datenträgern	☐ Verschlüsselung von Dateien
☐ Virtual Private Networks (VPN)	☐ Elektronische Signatur
☐ Sonstiges:	

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

[3] Entsprechend den bestehenden technisch-organisatorischen Maßnahmen anpassen.
[4] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

☐ Protokollierung	☐ Dokumentenmanagement
☐ Sonstiges:	

C. VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

☐ Backup-Strategie (online/offline; on-site/off-site)	☐ Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
☐ Virenschutz	☐ Firewall
☐ Meldewege und Notfallpläne	☐ Security Checks auf Infrastruktur- und Applikationsebene
☐ Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum	☐ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☐ Sonstiges:	

Rasche **Wiederherstellbarkeit:**

☐ Ja	☐ Nein

D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen:

☐ Ja	☐ Nein

Incident-Response-Management:

☐ Ja	☐ Nein

Datenschutzfreundliche Voreinstellungen:

☐ Ja	☐ Nein

Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch:

☐ Eindeutige Vertragsgestaltung	☐ Formalisiertes Auftragsmanagement
☐ Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)	☐ Vorabüberzeugungspflicht
☐ Nachkontrollen	☐ Sonstiges:

3. TOMs – Aufbau und Dokumentation

- **Vertraulichkeit**

  nur Berechtigte dürfen Zugriff auf personenbezogene Daten haben

Beispiele: Schlüssel, Chipkarten, Portier, Alarmanlage, Passwörter, Zwei-Faktor-Authentifizierung, Berechtigungsprofile, Protokollierung etc.

Anlage ./1 - Technisch-organisatorische Maßnahmen[3]

A. VERTRAULICHKEIT

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☐ Schlüssel	☐ Magnet- oder Chipkarten
☐ Elektrische Türöffner	☐ Portier
☐ Sicherheitspersonal	☐ Alarmanlagen
☐ Videoanlage	☐ Einbruchshemmende Fenster und/oder Sicherheitstüren
☐ Anmeldung beim Empfang mit Personenkontrolle	☐ Begleitung von Besuchern im Unternehmensgebäude
☐ Tragen von Firmen-/Besucherausweisen	☐ Sonstiges:

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☐ Kennwörter (einschließlich entsprechender Policy)	☐ Verschlüsselung von Datenträgern
☐ Automatische Sperrmechanismen	☐ Sonstiges:
☐ Zwei-Faktor-Authentifizierung	

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☐ Standard-Berechtigungsprofile auf „need to know-Basis"	☐ Standardprozess für Berechtigungsvergabe
☐ Protokollierung von Zugriffen	☐ Sichere Aufbewahrung von Speichermedien
☐ Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten	☐ Datenschutzgerechte Wiederverwendung von Datenträgern
☐ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☐ Clear-Desk/Clear-Screen Policy
☐ Sonstiges:	

Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt:

☐ Ja	☐ Nein

Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

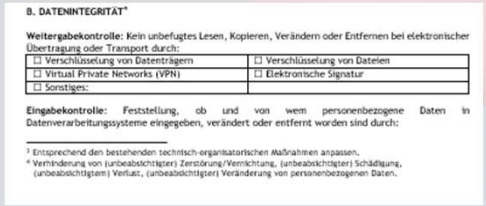
☐ Ja	☐ Nein

3. TOMs – Aufbau und Dokumentation

- **Integrität**

  Schutz vor unberechtigter Veränderung von personenbezogenen Daten

Beispiele: Elektronische Signatur, Verschlüsselung, VPN, Dokumentenmanagement, Protokollierung etc.



B. DATENINTEGRITÄT*

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☐ Verschlüsselung von Datenträgern	☐ Verschlüsselung von Dateien
☐ Virtual Private Networks (VPN)	☐ Elektronische Signatur
☐ Sonstiges:	

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

[3] Entsprechend den bestehenden technisch-organisatorischen Maßnahmen anpassen.
[4] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

☐ Protokollierung	☐ Dokumentenmanagement
☐ Sonstiges:	

3. TOMs – Aufbau und Dokumentation

Verfügbarkeit der Daten

- Schutz gegen Zerstörung und Verlust der Daten
  - Virenschutz, Firewall, Backup-Strategie, Redundanz
  - Feuer, Wasser, Blitz
- Notfallpläne, Meldewege (wer, wann, wie)
  - Geschäftsleitung, IT, Behörden, Kunden, Polizei, . . .

3. TOMs – Aufbau und Dokumentation

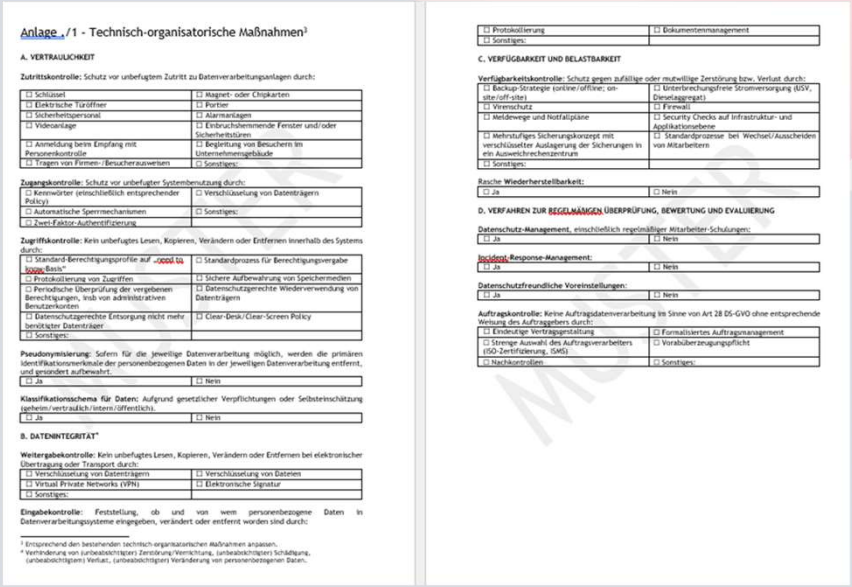
Belastbarkeit und Wiederherstellbarkeit des Systems

- Security-Checks, Monitoring
- Skalierbarkeit
- Datenarchivierung von alten Daten
- Updates und Patches

3. TOMs – Aufbau und Dokumentation

Dokumentation der TOMs

- Es besteht Dokumentationspflicht
  - Verzeichnisse der Verarbeitungstätigkeiten, Auftragsverarbeitervertrag
- Checkliste
- Jährliches Audit (wer, wann, was, wie)



Anlage ./1 - Technisch-organisatorische Maßnahmen[1]

A. VERTRAULICHKEIT

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☐ Schlüssel	☐ Magnet- oder Chipkarten
☐ Elektrische Türöffner	☐ Portier
☐ Sicherheitspersonal	☐ Alarmanlagen
☐ Videoanlage	☐ Einbruchshemmende Fenster und/oder Sicherheitstüren
☐ Anmeldung beim Empfang mit Personenkontrolle	☐ Begleitung von Besuchern im Unternehmensgebäude
☐ Tragen von Firmen-/Besucherausweisen	☐ Sonstiges:

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☐ Kennwörter (einschließlich entsprechender Policy)	☐ Verschlüsselung von Datenträgern
☐ Automatische Sperrmechanismen	☐ Sonstiges:
☐ Zwei-Faktor-Authentifizierung	

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☐ Standard-Berechtigungsprofile auf „need to know-Basis"	☐ Standardprozess für Berechtigungsvergabe
☐ Protokollierung von Zugriffen	☐ Sichere Aufbewahrung von Speichermedien
☐ Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten	☐ Datenschutzgerechte Wiederverwendung von Datenträgern
☐ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☐ Clear-Desk/Clear-Screen Policy
☐ Sonstiges:	

Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

☐ Ja	☐ Nein

Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☐ Ja	☐ Nein

B. DATENINTEGRITÄT*

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☐ Verschlüsselung von Datenträgern	☐ Verschlüsselung von Dateien
☐ Virtual Private Networks (VPN)	☐ Elektronische Signatur
☐ Sonstiges:	

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

[1] Entsprechend den bestehenden technisch-organisatorischen Maßnahmen anpassen.
* Veränderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

☐ Protokollierung	☐ Dokumentenmanagement
☐ Sonstiges:	

C. VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

☐ Backup-Strategie (online/offline; on-site/off-site)	☐ Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
☐ Virenschutz	☐ Firewall
☐ Meldewege und Notfallpläne	☐ Security Checks auf Infrastruktur- und Applikationsebene
☐ Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum	☐ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☐ Sonstiges:	

Rasche **Wiederherstellbarkeit:**

☐ Ja	☐ Nein

D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen:

☐ Ja	☐ Nein

Incident-Response-Management:

☐ Ja	☐ Nein

Datenschutzfreundliche Voreinstellungen:

☐ Ja	☐ Nein

Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch:

☐ Eindeutige Vertragsgestaltung	☐ Formalisiertes Auftragsmanagement
☐ Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)	☐ Vorabüberzeugungspflicht
☐ Nachkontrollen	☐ Sonstiges:

4. TOMs – Mitarbeiter

Schulung der Mitarbeiter

- Sensibilisierung für das Thema Datenschutz
- Verständnis für das Thema
- Begriffsbestimmung
- Verschlüsselung von Daten

4. TOMs – Mitarbeiter

Regelungen/Richtlinien

- Arbeitsvertrag, Verschwiegenheitserklärung
- Arbeitsplatzbeschreibung
- Datenminimierung
- Information über die Verarbeitung der MA-Daten
- Einverständniserklärung bei bestimmten Datenverarbeitungen

  (z.B. priv. Tel., Notfallnummern, Behinderung oder wenn Bilder der MA auf der Website aufscheinen)

4. TOMs – Mitarbeiter

Fremdpersonal

- Zugangskontrolle
- Zugriffskontrolle
- Auftragsverarbeitervertrag
- Verschwiegenheitserklärung

4. TOMs – Mitarbeiter

Entsorgung von Papier/Datenträgern

- Schredder

4. TOMs – Mitarbeiter

Umgang mit verdächtigen E-Mails

- Sinnhaftigkeit des Inhaltes überprüfen
- Check der Absenderadresse
- Bei Unsicherheiten – Rücksprache
- Als Spam markieren, Absender sperren, IT informieren

4. TOMs – Mitarbeiter

Home Office und der Umgang mit Firmengeräten

- Vertraglich festlegen, welche Geräte für welchen Zweck verwendet werden
- Zugriff auf Unternehmensressourcen sichern
- Kommunikationskanäle festlegen, Arbeitszeiten/Erreichbarkeit
- Orte festlegen (Wohnort, mobil, Ausland)
- Sicheres W-Lan, sichere Passwörter, Sicherheitssoftware, auch aufs Handy gehört ein Virenschutz, VPN, Firewall
- IT-Support zu Verfügung stellen

6. TOMs – Fragen

Hinweis

Alle Informationen in diesem Vortrag sind nach bestem Wissen und Gewissen zusammengestellt.

Der Vortragende weist jedoch darauf hin, dass keine Haftung für die Richtigkeit, Aktualität und Vollständigkeit übernommen wird.

Insbesondere ersetzt dieser Vortrag keine rechtliche, organisatorische oder technische Beratung im Einzelfall.

Die Präsentation stellt das Thema auszugsweise dar und bildet nur mit den mündlichen Ausführungen des Referenten eine entsprechende Einheit.

Jede Weitergabe der Unterlagen ohne Zustimmung des Referenten ist unzulässig!

Kontakte

DDSB.AT Beratung GmbH

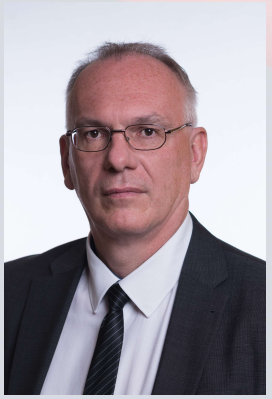
Mag. Günther Zikulnig

+43 1 4200050
office@ddsb.at
www.ddsb.at

IHS e.U.

Ing. Hannes Strasser

+43 664 1393935
strassert@ihs-beratung.at
www.ihs-beratung.at



Die ID-Austria

Fakten und Stolpersteine, STAND 15-05-24

Wir haben eine neue Signatur….

- „ID Austria mit Basisfunktion“ hat den Funktionsumfang der alten “Handysignatur”
- Die ID Austria mit Basisfunktion behält ebenfalls die Gültigkeitsdauer Ihrer Handy-Signatur, kann aber nicht mehr verlängert werden.
- Die normale ID Austria ist die Vollversion.
- Für den digitalen Führerschein und dergleichen wird Vollversion benötigt.
- Der digitale Führerschein kann nur genutzt werden, wenn man einen Scheckkartenführerschein hat.

Übersicht

Self-Service Funktionen

Neuen Fido-Token verknüpfen
Neues Smartphone verknüpfen
Verknüpfte Geräte verwalten
Signatur-Passwort ändern
Zertifikat verlängern

Ablage

Signierte Dokumente
A-Trust
Papierkorb

EPREL Dokumente

eTresor

Inbox
A-Trust
DSGVO-Scout
Unterschriftenmappe Archiv

Herzlich willkommen, Walter Wratschko

Quick-Sign

Hochladen und signieren

Dokumente hier ablegen oder Dateien durch klicken auswählen

Zertifikat

Gültig bis: 9.10.2028, 08:45

Zertifikatseriennummer: 1189264880

Produkt: ID Austria Full

CIN: 328330874051

Dokumente

Anzahl Dateien
1
Dateien in Signierte Dokumente
0
Verbrauchter Speicher
0.04 MB / 2 GB

Tipp: Die Ordner in der Menüleiste auf der linken Seite können per Drag & Drop umstrukturiert werden. Die Sortierung bleibt aber immer alphabetisch.

1 / 3

English

Wie komme ich zur Vollversion?

- Wurde die Handy-Signatur behördlich registriert, kann man selbst zur Vollversion der ID Austria aufrüsten.
- *Dazu wird man beim Anmeldevorgang gebeten, die Ausweisnummer (Pass, Führerschein) einzugeben, mit der man sich damals registriert hat.*

Wenn mein Registrar keine Behörde war…

- Auf oesterreich.gv.at/id-austria/registrierungsbehoerden.html gibt es eine Liste der Registrierungsbehörden.
- Zum Termin nimmt man das **Smartphone** mit, einen amtlichen **Lichtbildausweis** und ***ein Passfoto.***
- Nach der Identitätsfeststellung schickt die Behörde ein Einmalkennwort (TAN) **an die App**, welches man der Behördenmitarbeiter*in mitteilt.
- Danach werden in der App die Zustimmungen zur Nutzung von ID Austria erteilt und dies mit Gesichts- oder Fingerabdruckscan bestätigt.
- Ab jetzt kann man in der App den Punkt „Ausweise“ auswählen.
- Dort wird man aufgefordert, die App „eAusweise“ herunterzuladen. In dieser befindet sich der digitale Führerschein, der als QR-Code vorgezeigt werden kann.

Wer die APP nicht verwenden möchte:

- FIDO-Sicherheitsschlüssel können als zweiter Authentifizierungsfaktor zur Anmeldung mit ID Austria im Webbrowser verwendet werden und stellen dort eine Alternative zu Smartphone-Apps wie „Digitales Amt“ dar. Es handelt sich dabei um einen FIDO2 Token (Fast IDentity Online Token).
- **zum Beispiel:** Yubico YubiKey FIPS Serie
- mobile Telefonnummer notwendig für den SMS-TAN

Services

Neue digitale Amtsservices

Diese Dienste können Sie direkt hier auf oesterreich.gv.at nutzen:

Wohnsitz ändern
Anmeldung eines neuen Wohnsitzes, Ab- bzw. Ummeldung des bisherigen

Wahlkarte beantragen
Dieses Service ist innerhalb der Antragsfristen verfügbar

Urkunde beantragen
Bestellung von Auszügen aus dem ZPR, z.B. bei Verlust Ihrer Geburtsurkunde

Schwangerschaft & Geburt
Aufgabenliste anlegen und Erstausstellung der Urkunden für Ihr Kind beantragen

Reisepass ablegen
Sicheres Hinterlegen und automatische Erinnerung

PDF Signatur – Ein Service der App "Digitales Amt"
Digitale Unterschriften direkt am Smartphone erstellen und prüfen

PDF Signatur – Services
PDFs online unterschreiben und prüfen

Weitere Services

Diese Services können Sie – wenn Sie schon bei oesterreich.gv.at eingeloggt sind – ohne nochmalige Identifizierung nutzen.

- **Formularservice**
- **Bundesschatz**
- **Mein Postkorb**
- **Meldebestätigung**
- **Meldeauskunft**
- **Strafregisterbescheinigung**
- **Aktuelle Volksbegehren**
- **Brutto-Netto-Rechner (inkl. Familienbonus Plus)**
- **Justiz Formulare**
- **Diebstahlsanzeige**
- **ZVR E-Gov-Beauftragter**
- **Pendlerrechner**
- **Geburtsanzeige / Todesanzeige**
- **Zentrales Waffenregister**
- **Online-Terminvereinbarung (BMI)**

Mit der Vollversion können wir….

- **ID-Austria verlängern…**
  - Ist nicht automatisch vorgesehen…
  - Ausländer:innen können nicht in der APP verlängern (3 Jahre / Mit Wohnsitz in Ö: 5 Jahre)
- Zusätzliches ID-Austria Konto erstellen (beruflich/privat)
- ID-Austria sperren bzw. widerrufen
- Verwendungsverlauf einsehen

ING. WALTER WRATSCHKO

EXPERTE FÜR BRÜSSELER IT-SPITZEN,
DATENSCHUTZ-KOORDINATOR & - BEAUFTRAGTER,
SCOUT FÜR EINE SMARTE KI

OFFICE KLAGENFURT: BRUNNPLATZ 5, 9020,
T: +43 699 1504 3860
E: WALTER.WRATSCHKO@DATENSCHUTZ-SUED.AT
I: WWW.MYPERFECT.IT

Ich danke für die Aufmerksamkeit!

Terminaviso

Nächste Folge „1 Stunde Datenschutz“ am **26. Juni 2024** von 09:00 bis 10:30 Uhr

Thema: NIS2