AGAD Service GmbH – Ihre Daten unser Schutz –

AGAD

Partner im Wettbewerb.

DATENSCHUTZ ZUM FEIERABEND

„Pflichtdokumentation leicht gemacht!“

Vorstellung des neuen VVT-Tools

der AGAD Service GmbH

RA Moritz Hudy

22. September 2022

AGAD
Partner im Wettbewerb.

Die Themen:

I. Verarbeitungsverzeichnisse nach der DS-GVO

1. Was sind Verarbeitungsverzeichnisse?
2. Wer muss Verarbeitungsverzeichnisse führen?
3. Welchen Inhalt müssen Verarbeitungsverzeichnisse haben?
4. Was droht bei Verstößen?

II. Das VVT-Tool der AGAD Service GmbH

1. Funktionen
2. Beispiele
3. Einführung

AGAD
Partner im Wettbewerb.

Was sind Verarbeitungsverzeichnisse?

Art. 30 I 1 DS-GVO:

Verzeichnis aller Verarbeitungstätigkeiten, die der Zuständigkeit der verantwortlichen Stelle unterliegen.

Verarbeitung: Alle Prozesse im Unternehmen, bei denen personenbezogene Daten im Unternehmen erhoben, gespeichert, verändert, übermittelt, gesperrt oder gelöscht werden.

AGAD
Partner im Wettbewerb.

Wer muss Verarbeitungsverzeichnisse führen?

Art. 30 I 1 DS-GVO:

Jede verantwortliche Stelle

→ **Also jedes Unternehmen (Art. 4 Nr. 7 DS-GVO)**

Ausnahme Art. 30 V DS-GVO:

Ein Unternehmen mit weniger als 250 Mitarbeitern ist in folgenden Fällen von der Pflicht befreit: Datenverarbeitung birgt kein Risiko für die Rechte und Freiheiten der Betroffenen, Datenverarbeitung erfolgt gelegentlich, keine Datenverarbeitung von besonderen Kategorien von personenbezogenen Daten im Sinne von Art. 9 Abs. 1 DSGVO und Art. 10 DSGVO.

→ In der Praxis kaum Bedeutung!

AGAD
Partner im Wettbewerb.

Welchen Inhalt müssen Verarbeitungsverzeichnisse haben?

Name und Kontaktdaten des Verantwortlichen	Zweck der Verarbeitung
Rechtsgrundlage der Verarbeitung	Datenkategorien
Auflistung der Betroffenen	(Kategorien von) Datenempfänger und Drittlandempfänger
Löschfristen	Getroffene technische und organisatorische Maßnahmen (TOM)

AGAD
Partner im Wettbewerb.

Was droht bei Verstößen?

Führt ein Unternehmen kein Verzeichnis von Verarbeitungstätigkeiten und/oder stellt dieses der Behörde nicht vollständig bereit, droht nach Art. 83 Abs. 4 a EU-DSGVO ein Bußgeld.

Bußgeldrahmen: Bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes

AGAD
Partner im Wettbewerb.

Das neue VVT-Tool der AGAD Service GmbH bietet eine einfache Möglichkeit zur Umsetzung der gesetzlichen Dokumentationsverpflichtungen

Das neue VVT-Tool der AGAD Service GmbH

→Eigener Bereich für das Unternehmen zum Erstellen und Pflegen der Verfahrensverzeichnisse und der TOMs (technische und organisatorischen Maßnahmen)

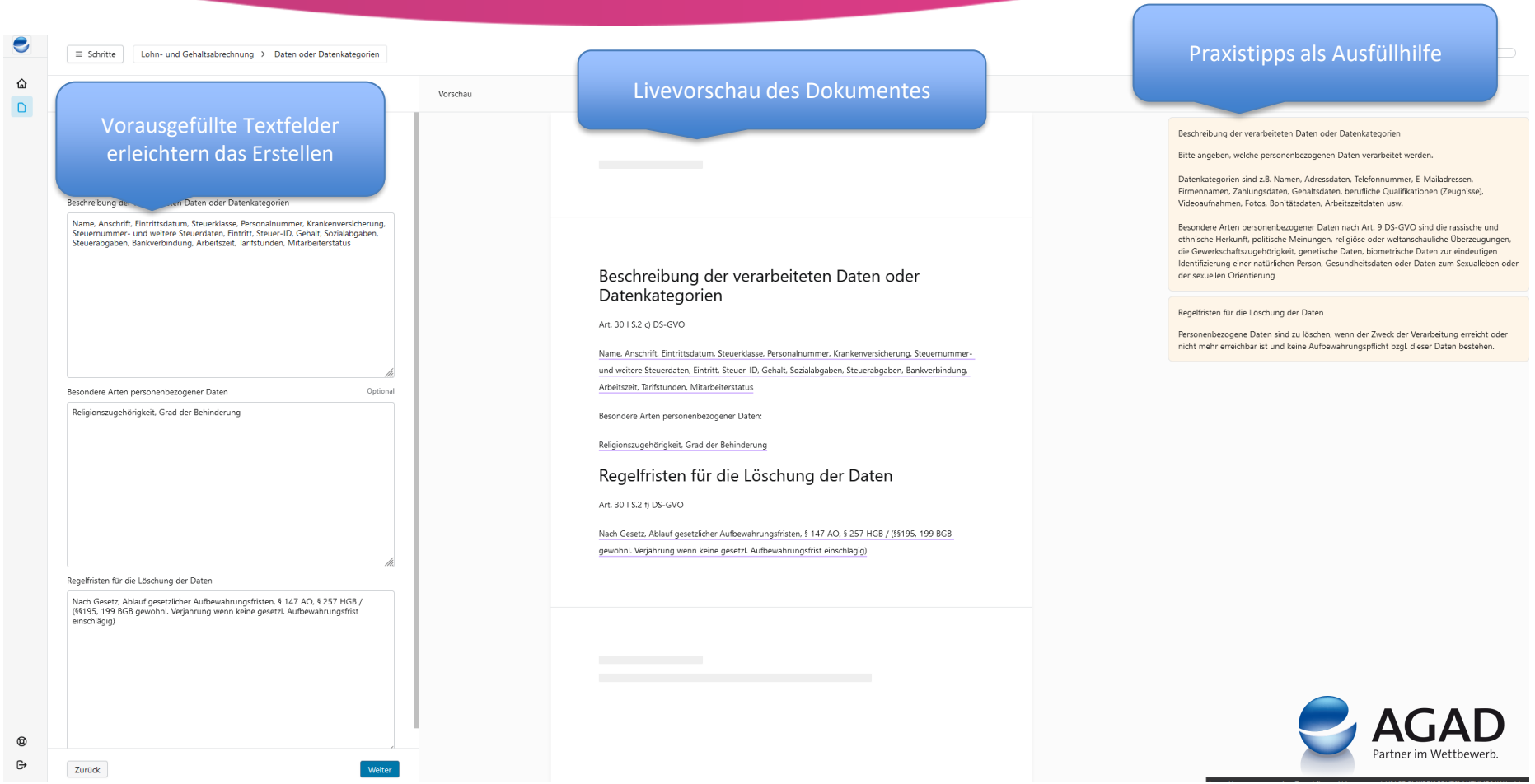
→Kontrolle und Unterstützung beim Erstellen der Verfahrensverzeichnisse durch den zuständigen Sachbearbeiter

→Einfaches Erstellen durch vorausgefüllte Dokumente, die aber auch vollständig angepasst werden können

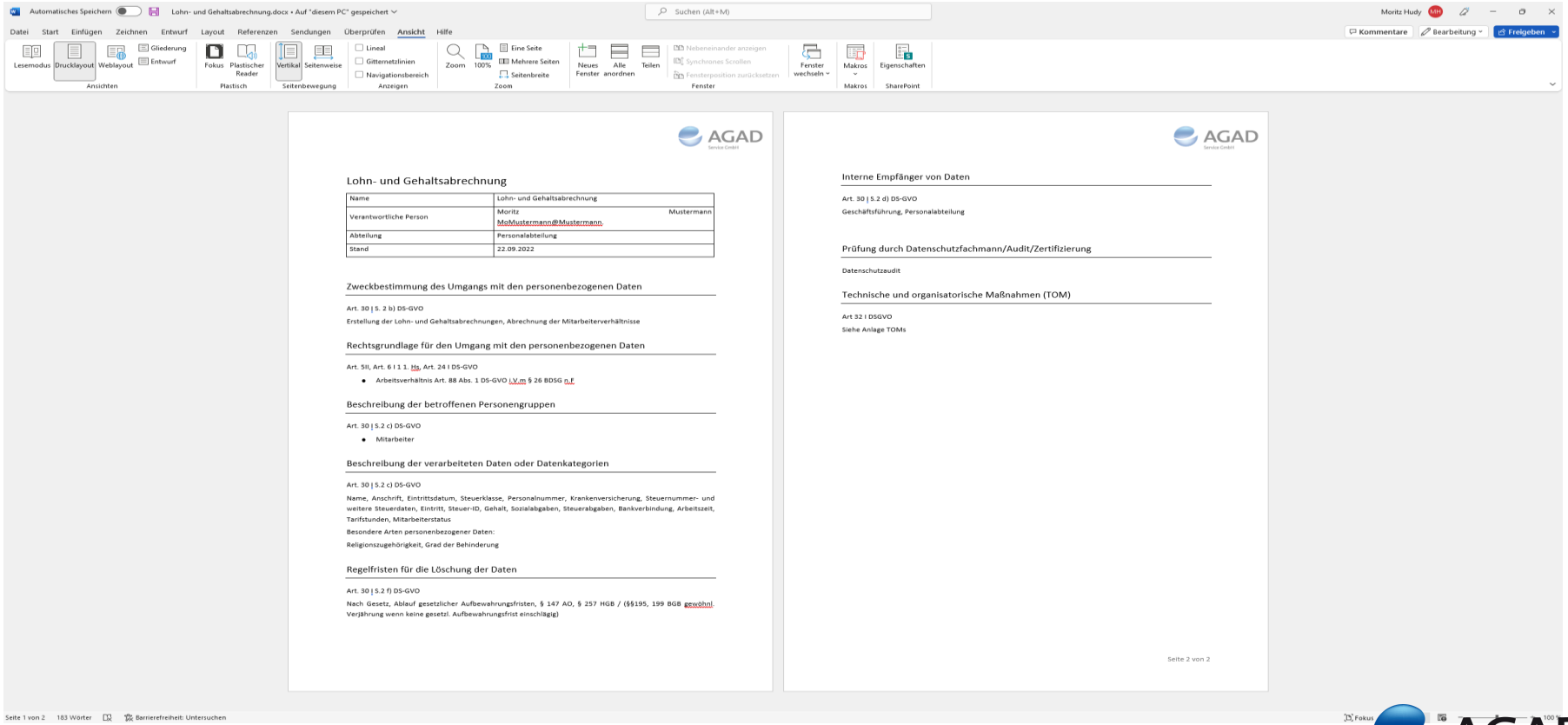
→Export der Dokumente für die eigene Dokumentation

AGAD
Partner im Wettbewerb.

Das VVT-Tool der AGAD Service GmbH



Das VVT-Tool der AGAD Service GmbH



Lohn- und Gehaltsabrechnung

Name	Lohn- und Gehaltsabrechnung
Verantwortliche Person	Moritz Mustermann MoMustermann@Mustermann.
Abteilung	Personalabteilung
Stand	22.09.2022

Zweckbestimmung des Umgangs mit den personenbezogenen Daten

Art. 30 | 5. 2 b) DS-GVO

Erstellung der Lohn- und Gehaltsabrechnungen, Abrechnung der Mitarbeiterverhältnisse

Rechtsgrundlage für den Umgang mit den personenbezogenen Daten

Art. 5II, Art. 6 I 1 1. Hs, Art. 24 I DS-GVO

- Arbeitsverhältnis Art. 88 Abs. 1 DS-GVO i.V.m § 26 BDSG n.F.

Beschreibung der betroffenen Personengruppen

Art. 30 | 5.2 c) DS-GVO

- Mitarbeiter

Beschreibung der verarbeiteten Daten oder Datenkategorien

Art. 30 | 5.2 c) DS-GVO

Name, Anschrift, Eintrittsdatum, Steuerklasse, Personalnummer, Krankenversicherung, Steuernummer- und weitere Steuerdaten, Eintritt, Steuer-ID, Gehalt, Sozialabgaben, Steuerabgaben, Bankverbindung, Arbeitszeit, Tarifstunden, Mitarbeiterstatus

Besondere Arten personenbezogener Daten:

Religionszugehörigkeit, Grad der Behinderung

Regelfristen für die Löschung der Daten

Art. 30 | 5.2 f) DS-GVO

Nach Gesetz, Ablauf gesetzlicher Aufbewahrungsfristen, § 147 AO, § 257 HGB / (§§195, 199 BGB gewöhnl. Verjährung wenn keine gesetzl. Aufbewahrungsfrist einschlägig)

Interne Empfänger von Daten

Art. 30 | 5.2 d) DS-GVO

Geschäftsführung, Personalabteilung

Prüfung durch Datenschutzfachmann/Audit/Zertifizierung

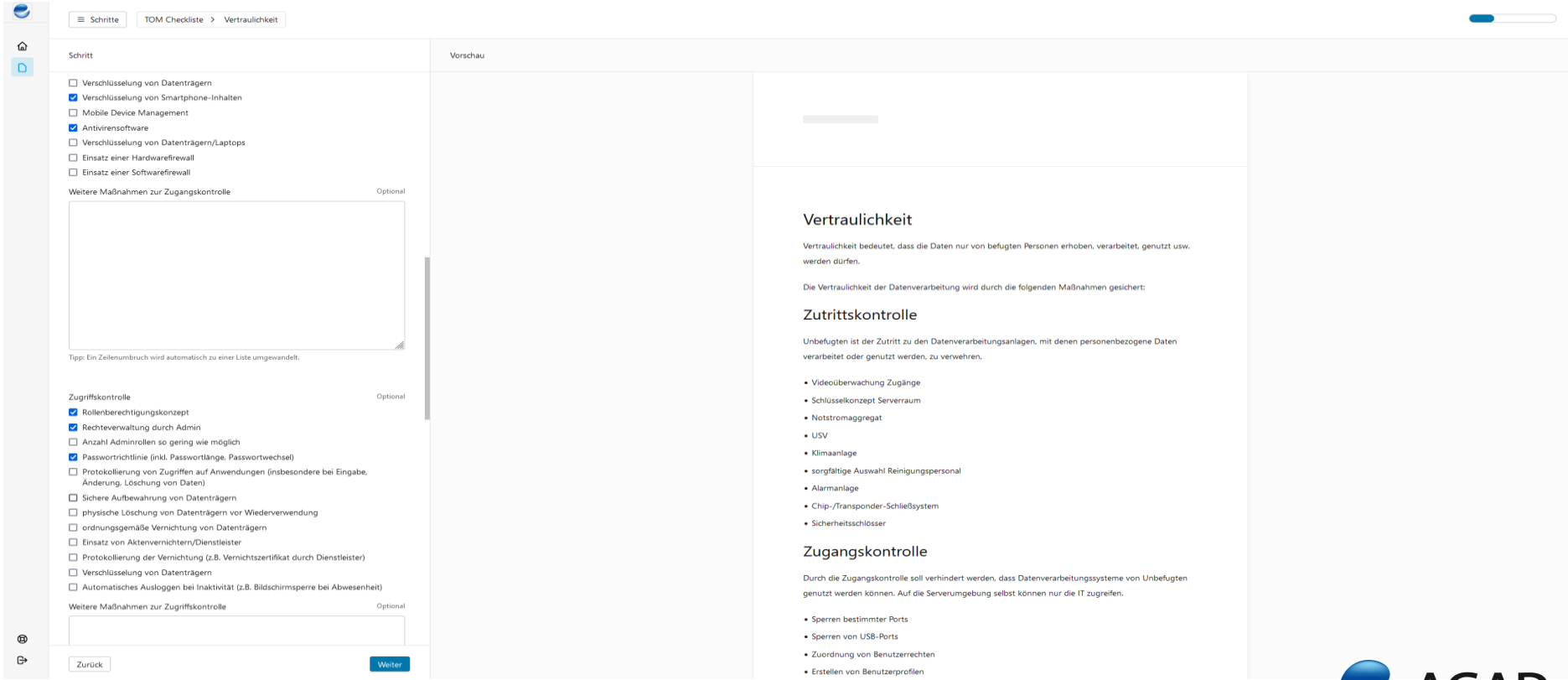
Datenschutzaudit

Technische und organisatorische Maßnahmen (TOM)

Art 32 I DSGVO

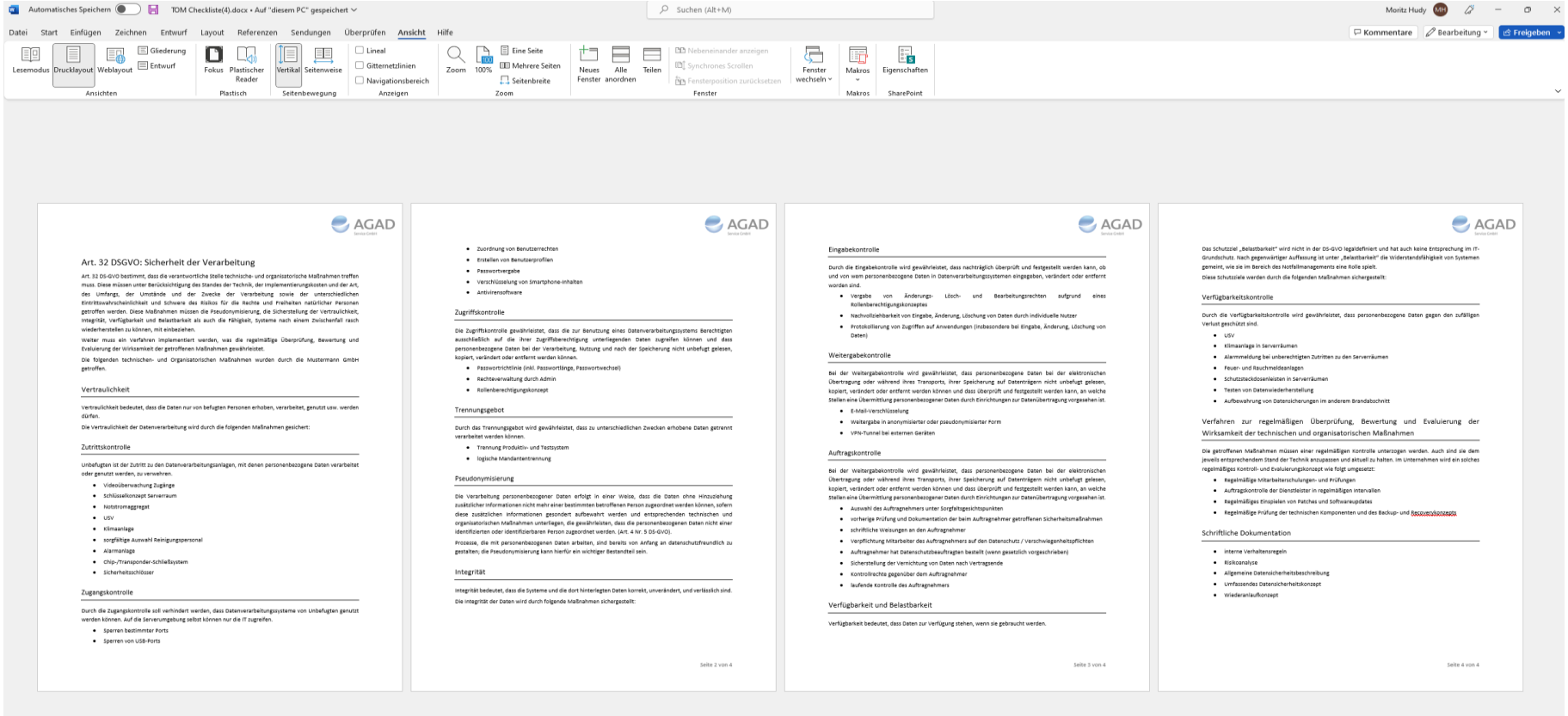
Siehe Anlage TOMs

AGAD
Partner im Wettbewerb.



AGAD
Partner im Wettbewerb.

Das VVT-Tool der AGAD Service GmbH



Automatisches Speichern — TOM Checkliste(4).docx • Auf "diesem PC" gespeichert — Suchen (Alt+M) — Moritz Hudy

Datei Start Einfügen Zeichnen Entwurf Layout Referenzen Sendungen Überprüfen Ansicht Hilfe — Kommentare — Bearbeitung — Freigeben

Lesemodus Drucklayout Weblayout Gliederung Entwurf — Ansichten
Fokus Plastischer Reader — Plastisch
Vertikal Seitenweise — Seitenbewegung
Lineal Gitternetzlinien Navigationsbereich — Anzeigen
Zoom 100% Eine Seite Mehrere Seiten Seitenbreite — Zoom
Neues Fenster Alle anordnen Teilen Nebeneinander anzeigen Synchrones Scrollen Fensterposition zurücksetzen Fenster wechseln — Fenster
Makros — Makros
Eigenschaften — SharePoint

AGAD

Art. 32 DSGVO: Sicherheit der Verarbeitung

Art. 32 DS-GVO bestimmt, dass die verantwortliche Stelle technische- und organisatorische Maßnahmen treffen muss. Diese müssen unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen getroffen werden. Diese Maßnahmen müssen die Pseudonymisierung, die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit als auch die Fähigkeit, Systeme nach einem Zwischenfall rasch wiederherstellen zu können, mit einbeziehen.
Weiter muss ein Verfahren implementiert werden, was die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen gewährleistet.
Die folgenden technischen- und Organisatorischen Maßnahmen wurden durch die Mustermann GmbH getroffen.

Vertraulichkeit

Vertraulichkeit bedeutet, dass die Daten nur von befugten Personen erhoben, verarbeitet, genutzt usw. werden dürfen.
Die Vertraulichkeit der Datenverarbeitung wird durch die folgenden Maßnahmen gesichert:

Zutrittskontrolle

Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Videoüberwachung Zugänge
- Schlüsselkonzept Serverraum
- Notstromaggregat
- USV
- Klimaanlage
- sorgfältige Auswahl Reinigungspersonal
- Alarmanlage
- Chip-/Transponder-Schließsystem
- Sicherheitsschlösser

Zugangskontrolle

Durch die Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Auf die Serverumgebung selbst können nur die IT zugreifen.

- Sperren bestimmter Ports
- Sperren von USB-Ports

AGAD

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Verschlüsselung von Smartphone-Inhalten
- Antivirensoftware

Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Passwortrichtlinie (inkl. Passwortlänge, Passwortwechsel)
- Rechteverwaltung durch Admin
- Rollenberechtigungskonzept

Trennungsgebot

Durch das Trennungsgebot wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung Produktiv- und Testsystem
- logische Mandantentrennung

Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugeordnet werden. (Art. 4 Nr. 5 DS-GVO).
Prozesse, die mit personenbezogenen Daten arbeiten, sind bereits von Anfang an datenschutzfreundlich zu gestalten; die Pseudonymisierung kann hierfür ein wichtiger Bestandteil sein.

Integrität

Integrität bedeutet, dass die Systeme und die dort hinterlegten Daten korrekt, unverändert, und verlässlich sind.
Die Integrität der Daten wird durch folgende Maßnahmen sichergestellt:

AGAD

Eingabekontrolle

Durch die Eingabekontrolle wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

- Vergabe von Änderungs- Lösch- und Bearbeitungsrechten aufgrund eines Rollenberechtigungskonzeptes
- Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten durch individuelle Nutzer
- Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung, Löschung von Daten)

Weitergabekontrolle

Bei der Weitergabekontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- E-Mail-Verschlüsselung
- Weitergabe in anonymisierter oder pseudonymisierter Form
- VPN-Tunnel bei externen Geräten

Auftragskontrolle

Bei der Weitergabekontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer
- Verpflichtung Mitarbeiter des Auftragnehmers auf den Datenschutz / Verschwiegenheitspflichten
- Auftragnehmer hat Datenschutzbeauftragten bestellt (wenn gesetzlich vorgeschrieben)
- Sicherstellung der Vernichtung von Daten nach Vertragsende
- Kontrollrechte gegenüber dem Auftragnehmer
- laufende Kontrolle des Auftragnehmers

Verfügbarkeit und Belastbarkeit

Verfügbarkeit bedeutet, dass Daten zur Verfügung stehen, wenn sie gebraucht werden.

AGAD

Das Schutzziel „Belastbarkeit" wird nicht in der DS-GVO legaldefiniert und hat auch keine Entsprechung im IT-Grundschutz. Nach gegenwärtiger Auffassung ist unter „Belastbarkeit" die Widerstandsfähigkeit von Systemen gemeint, wie sie im Bereich des Notfallmanagements eine Rolle spielt.
Diese Schutzziele werden durch die folgenden Maßnahmen sichergestellt:

Verfügbarkeitskontrolle

Durch die Verfügbarkeitskontrolle wird gewährleistet, dass personenbezogene Daten gegen den zufälligen Verlust geschützt sind.

- USV
- Klimaanlage in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu den Serverräumen
- Feuer- und Rauchmeldeanlagen
- Schutzsteckdosenleisten in Serverräumen
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherungen im anderem Brandabschnitt

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die getroffenen Maßnahmen müssen einer regelmäßigen Kontrolle unterzogen werden. Auch sind sie dem jeweils entsprechendem Stand der Technik anzupassen und aktuell zu halten. Im Unternehmen wird ein solches regelmäßiges Kontroll- und Evaluierungskonzept wie folgt umgesetzt:

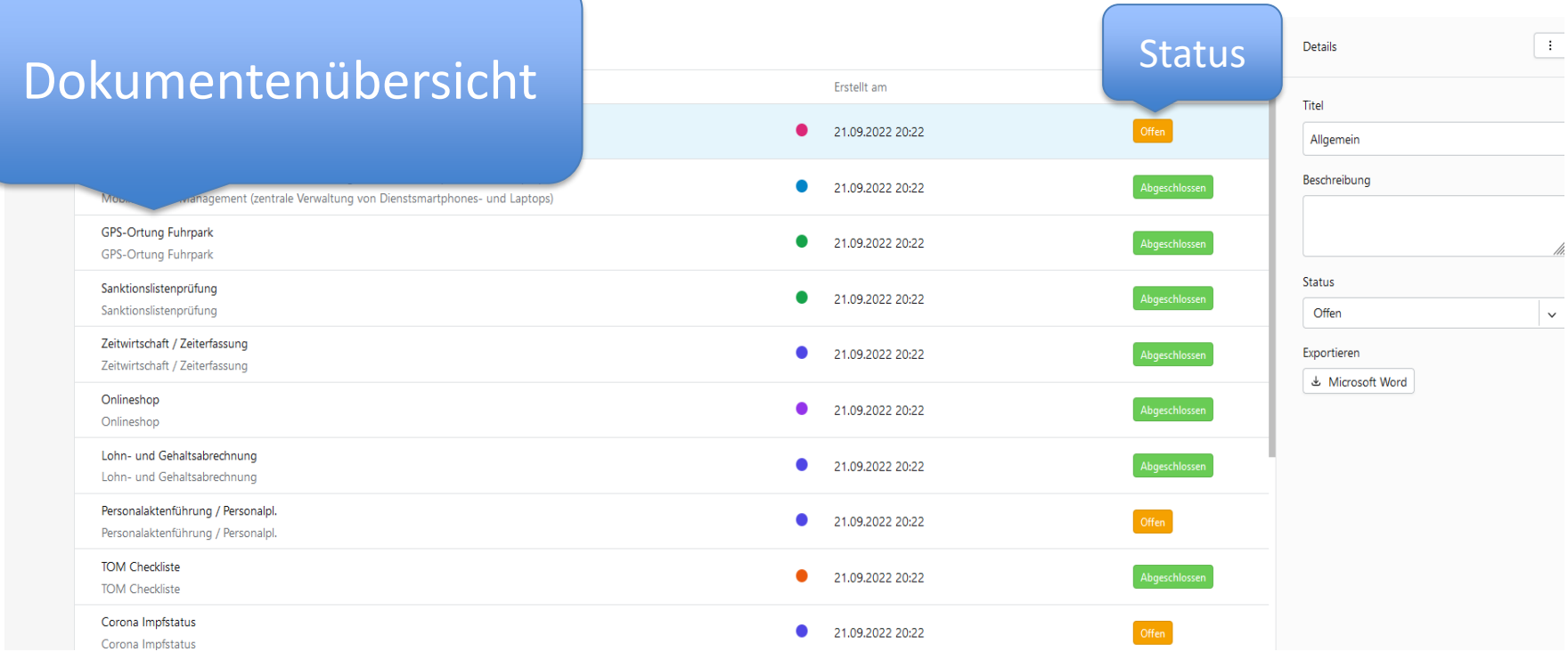
- Regelmäßige Mitarbeiterschulungen- und Prüfungen
- Auftragskontrolle der Dienstleister in regelmäßigen Intervallen
- Regelmäßiges Einspielen von Patches und Softwareupdates
- Regelmäßige Prüfung der technischen Komponenten und des Backup- und Recoverykonzepts

Schriftliche Dokumentation

- Interne Verhaltensregeln
- Risikoanalyse
- Allgemeine Datensicherheitsbeschreibung
- Umfassendes Datensicherheitskonzept
- Wiederanlaufkonzept

Dokumentenübersicht

Status



Ablauf

Erfassung der Verfahren über eine Checkliste → Einladung zur Anmeldung und Freischaltung der Vorlagen → Ausfüllen der Dokumente → Kontrolle durch Juristen der AGAD Service GmbH

= gesetzliche Verpflichtung erfüllt ☑

Das Beste zum Schluss

Einführung für Kunden der AGAD Service GmbH kostenlos im Zuge des

jährlichen Datenschutzaudits

Nutzung für Mitglieder des AGAD e.V. zu exklusiven Konditionen

AGAD
Partner im Wettbewerb.

Herzlichen Dank
für Ihre Aufmerksamkeit!

AGAD Service GmbH
RA Moritz Hudy
Waldring 43-47
44789 Bochum
hudy@agad.de
Tel.: 0234/282533 20

AGAD
Partner im Wettbewerb.