Bewertung der technisch-organisatorischen Maßnahmen der Team Management Services GmbH bei der Erbringung von beauftragten Leistungen gem. Art. 28 (3) lit.c DSGVO

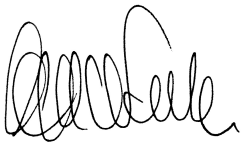
Zweck dieses Dokuments:

Um Auftraggebern von Supportleistungen für die Durchführung von Trainings unter Verwendung von s.g. Team Management Profilen einen Überblick über die spezifischen technischen und organisatorischen Maßnahmen bei der Team Management GmbH (im Weiteren „TMS GmbH“) zu geben, werden einzelne beauftragte Prozessschritte auf ihre Risiken für die Betroffenen hin untersucht, sowie die Wirksamkeit getroffener Maßnahmen zur Minderung der Risiken bewertet.

Hier nicht bewertet werden die allgemeinen technischen und organisatorischen Maßnahmen, so wie sie in der Vorlage zum TMS AV Vertrag in der Anlage beschrieben sind.

Das in diesem Dokument verwendete Trainingsszenario entspricht dem Beispiel 1. Trainer ohne eigene TMP Lizenz des TMS Dokuments Datenschutzhandbuch TMS Trainer.

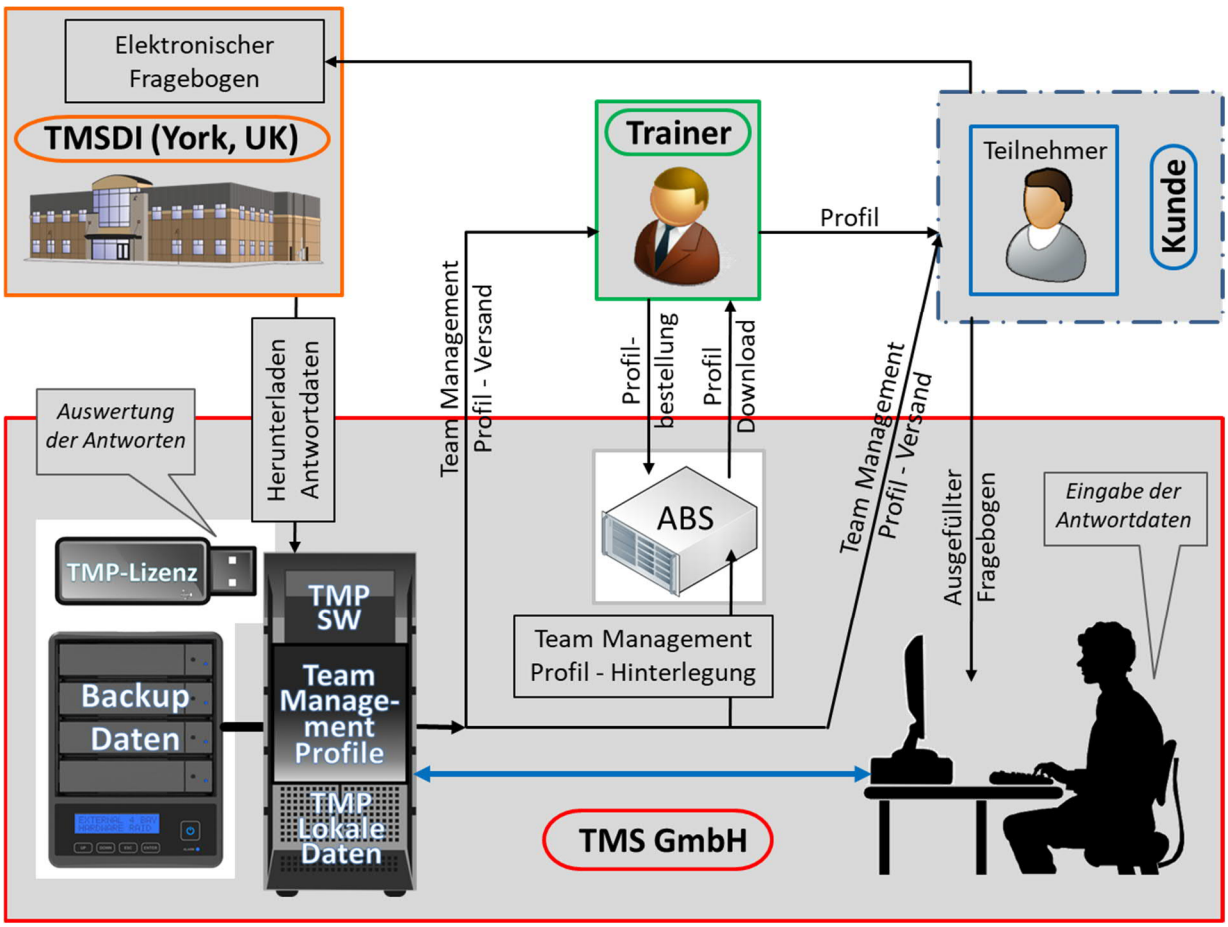
Freiburg, 06.04.2023



Digital signiert von Reinhard M. Novak
DN: cn=Reinhard M. Novak, email=kontakt@dsb-ext.com
Datum: 2023.04.06 16:13:49 +02'00'

Reinhard M. Novak
(Verantwortlich für die datenschutzrechtliche Bewertung)

Inanspruchnahme der TMS Dienstleistung über einen akkreditierten Trainer, der keine eigene Lizenz zur Nutzung der TMP Software für die Erstellung der TMS® Profile hat.



1. Bereitstellung des Systems ABS (profilbestellung.de) für die Organisation des Trainings

Das System ABS wird dem Trainer auftragsgemäß von der TMS GmbH zur Verfügung gestellt. Für die Zwecke der Organisation des Trainings wird es ausschließlich vom Trainer genutzt. ABS ist unter der Adresse https://www.profilbestellung.de/ verfügbar.

Seq.	Art der Daten	Verarbeitet durch	Kommentar bzw. Bewertung (TMS GmbH & ext. DSB)
1.1	Benutzer-verwaltung	TMS GmbH	Die Benutzerverwaltung auf profilbestellung.de ist keine im Auftrag gem. Art.28 DSGVO erbrachte Leistung der TMS GmbH. Die Sicherheit der Benutzerverwaltung ist jedoch konstitutiv für die Sicherheit der auf diesem System durch den Trainer verarbeiteten Daten der Teilnehmer. Als beruflich Selbständiger ist der Trainer der datenschutzrechtlich Verantwortliche für die Durchführung von Trainings. Gehört der Trainer einem Unternehmen an, ist das Unternehmen, das den Trainer beschäftigt der datenschutzrechtlich Verantwortliche. Siehe dazu den *Abschnitt (3) Grundlegendes* im Datenschutzhandbuch für TMS Trainer. Beschäftigt ein Verantwortlicher mehrere TMS Trainer, können diese technisch zu einer Benutzergruppe zusammengefasst werden.

			Innerhalb dieser Benutzergruppe können Mitglieder ihre Zugriffsrechte auf Organisationsdaten für Trainings (siehe 1.2) oder auf zum Abruf hinterlegte Team Management Profile (siehe 6.4) an andere Gruppenmitglieder delegieren. Dies erlaubt dem Verantwortlichen (z.B. einem Trainingsunternehmen) die Rolle eines Assistenten festzulegen, welcher spezifische Aufgaben in Unterstützung der Trainer wahrnimmt. Im Folgenden wird eine Verarbeitung personenbezogener Daten durch einen Verantwortlichen der Einfachheit halber als Verarbeitung durch einen Trainer bezeichnet, unabhängig davon, ob der Verantwortliche eine Einzelperson oder ein Unternehmen ist.
	Risiken für die Betroffenen		a. Insofern es sich bei den Betroffenen um die Nutzer von profilbestellung.de handelt, sind die Risiken für die Vertraulichkeit und Integrität ihrer Daten gering bis mittel. b. Insofern es sich bei den Betroffenen um die Teilnehmer an TMS Trainingsmaßnahmen handelt, deren Daten von den Nutzern von profilbestellung.de verarbeitet werden, sind die Risiken insbesondere für die Vertraulichkeit ihrer Daten mittel bis hoch (siehe Abschnitt 6.4).
	Getroffene Maßnahmen		• Verifizierung der Identität jedes Antragstellers auf einen Zugang zu profilbestellung.de; bei verlangtem Reset des Passworts dient die E-Mail-Adresse des Antragstellers zur Verifikation. • Passwort-Regeln: Das Passwort muss mindestens 12 Zeichen lang sein und muss Großbuchstaben, Kleinbuchstaben, eine Zahl und eines der folgenden Sonderzeichen beinhalten "@$!%*#?&" . • Datentrennung, ein Trainer kann nur auf „seine“ Daten zugreifen. • Verifizierung der Berechtigung zur Mitgliedschaft in Nutzergruppen
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.
1.2	Kontaktdaten des Teilnehmers	Trainer	Hinterlegung der Kontaktdaten der Teilnehmer an einem Training, Überprüfung des Trainingsfortschritts Anforderungen für die Erstellung eines Team Management Profils pro Teilnehmer.
	Risiken für die Betroffenen		Vertraulichkeit & Integrität, geringes bis mittleres Risiko
	Getroffene Maßnahmen		Zugangskontrolle zu ABS durch individuelle Logins für jeden Trainer. Datentrennung, ein Trainer kann nur auf „seine“ Daten zugreifen.
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.
1.3	Profil-anforderungen	Eingabe durch Trainer	Anforderungen für die Erstellung eines Team Management Profils pro Teilnehmer.
	Risiken für die Betroffenen		Vertraulichkeit & Integrität, geringes bis mittleres Risiko
	Getroffene Maßnahmen		Zugangskontrolle zu ABS durch individuelle Logins für jeden Trainer. Datentrennung, ein Trainer kann nur auf „seine“ Daten zugreifen.
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.

2. Bereitstellung des elektronischen Fragebogens für die Selbsteinschätzung der Teilnehmer

Der elektronische Fragebogen wird dem Trainer auftragsgemäß von der TMS GmbH zur Verfügung gestellt. Die eigentliche Bereitstellung erfolgt durch den Unterauftragnehmer TMS DI (York). TMS DI (York) verarbeitet die Daten als „Software as a Service“ Dienstleister, also zu keinem Zeitpunkt für andere als die beauftragten Zwecke.

Die Antworten des Teilnehmers werden dem Speicherbereich des Trainers bzw. der TMS GmbH auf dem TMS DI Server zugeordnet.

Seq.	Art der Daten	Verarbeitet durch	Kommentar bzw. Bewertung (TMS GmbH & ext. DSB)
2.1	Kontakt- und Organisations-daten des Teilnehmers	TMS DI (York) im SaaS Auftrag des Trainers	Damit der Trainer die Team Management Profile dem Teilnehmer zuordnen kann, müssen zumindest pseudonyme Kontaktdaten angegeben werden. Darüber hinaus kann der Teilnehmer weitere Organisationsdaten angeben. Die datenschutzrechtliche Verantwortung für die Erhebung dieser Daten liegt, ebenso wie die für die Erhebung der Antwortdaten zu den Arbeitspräferenzen, beim Trainer, bzw. dem Unternehmen, dem der Trainer angehört.
	Risiken für die Betroffenen		Vertraulichkeit & Integrität, geringes bis mittleres Risiko
	Getroffene Maßnahmen		Zugangskontrolle zum TMS DI Server durch individuelle Logins für jeden Trainer, bzw. für zur Auswertung der Antwortdaten bei der TMS GmbH befugtes Personal. Datentrennung, ein Trainer kann nur auf „seine“ Daten zugreifen.
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.
2.2	Kodierte Antwortdaten des Teilnehmers	TMS DI (York) im Auftrag des Trainers	In diesem Prozessschritt gibt der Teilnehmer seine Selbsteinschätzung zu seinen Arbeitspräferenzen in einem Multiple Choice Fragebogen ein.
	Risiken für die Betroffenen		a. Vertraulichkeit & Integrität, geringes bis mittleres Risiko b. Begrenzung der Speicherdauer, geringes bis mittleres Risiko
	Getroffene Maßnahmen		a. Die Antwortdaten des Teilnehmers werden als Ziffernfolge gespeichert. Ohne die Verwendung der TMP-Auswertungssoftware für die Erstellung eines druckbaren Profils lassen die Antwortdaten keine Rückschlüsse auf die Antworten des Teilnehmers zu. b. Die in 2.1 und 2.2 genannten Daten werden spätestens nach 3 Monaten vollautomatisch vom Server der TMS DI gelöscht.
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.

3. Herunterladen der Antwortdaten vom TMS DI Server in das TMP System der TMS GmbH

Damit die kodierten Antwortdaten in ein lesbares Team Management Profil gebracht werden können, müssen sie mittels der TMP-Software ausgewertet werden. Zu diesem Zweck werden die in 2.1 und 2.2 genannten Daten durch die TMS GmbH vom TMS DI Server in das lokale TMP-System übertragen.

Seq.	Art der Daten	Verarbeitet durch	Kommentar bzw. Bewertung (TMS GmbH & ext. DSB)

3.1	Wie in 2.1 und 2.2	TMS GmbH im Auftrag des Trainers	
	Risiken für die Betroffenen		Vertraulichkeit & Integrität, geringes bis mittleres Risiko
	Getroffene Maßnahmen		Datentrennung nach Kunde bzw. Trainer/Trainingsunternehmen Speicherung der Antwortdaten als Ziffernfolge
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.

4. Eingabe der Antwortdaten eines schriftlichen Fragebogens durch die TMS GmbH in das TMP System der TMS GmbH

Die Daten eines vom Teilnehmer schriftlich ausgefüllten Fragebogens müssen für die Erstellung eines Team Management Profils in das lokale TMP-System eingegeben werden.

Seq.	Art der Daten	Verarbeitet durch	Kommentar bzw. Bewertung (TMS GmbH & ext. DSB)
4.1	Wie in 2.1 und 2.2	TMS GmbH im Auftrag des Trainers	
	Risiken für die Betroffenen		Vertraulichkeit & Integrität, hohes Risiko
	Getroffene Maßnahmen		Sofortige Vernichtung des schriftlichen Fragebogens nach der Eingabe der Antwortdaten
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.

5. Verarbeitungen der Antwortdaten im TMP System der TMS GmbH

Seq.	Art der Daten	Verarbeitet durch	Kommentar bzw. Bewertung (TMS GmbH & ext. DSB)
5.1	Wie in 2.1 und 2.2	TMS GmbH im Auftrag des Trainers	Auswertung und Profilerstellung Damit die Antwortdaten in ein les- bzw. druckbares Format, das s.g. Team Management Profil, gebracht werden können, müssen sie vom TMP System vollautomatisch ausgewertet werden. Jede Auswertung ist kostenpflichtig (siehe 1.2 oben, Lizenz-Count). Nach der Auswertung werden die Daten weiterhin als kodierte Ziffernfolge als „Profildaten“ gespeichert, jedoch entsprechend markiert, damit bei einer erneuten Erstellung des druckbaren Profils keine weitere Verrechnung erfolgt (kein Lizenz-Count).
	Risiken für die Betroffenen		Vertraulichkeit & Integrität, geringes bis mittleres Risiko
	Getroffene Maßnahmen		Zugang zur TMP Software nur für autorisiertes Personal.
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.
5.2	Wie in 2.1 und 2.2	TMS GmbH im Auftrag des Trainers	Weitere Speicherung der Profildaten entsprechend dem Auftrag durch den Trainer.
	Risiken für die Betroffenen		a. Vertraulichkeit & Integrität, geringes bis mittleres Risiko b. Begrenzung der Speicherdauer, geringes Risiko
	Getroffene Maßnahmen		a. Zugang zur TMP Software nur für autorisiertes Personal. Hohe Anforderung an die Komplexität des Passworts. Vereinfachter Zugang ist über einen auf den Mitarbeiter bezogenen USB Stick als "Dongle" mit PIN für USB-Login möglich.

			b. Automatisierte Löschung nach der vom Trainer vorgegebenen Speicherdauer (in der Regel 5 Jahre)
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.
5.3	Wie in 2.1 und 2.2	TMS GmbH im Auftrag des Trainers	Anonymisierung der Profildaten vor dem Transfer an ITMS Brisbane
	Risiken für die Betroffenen		Vertraulichkeit, sehr geringes bis kein Risiko
	Getroffene Maßnahmen		Der Vorgang der Anonymisierung wird regelmäßig geprüft, das Ergebnis der aktuellen Prüfung auf der Webseite für akkreditierte TMS Trainer veröffentlicht.
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.

6. Übergabe der Team Management Profile an den Trainer bzw. den Teilnehmer

Das mit einer Übergabe der Team Management Profile an den Trainer bzw. den Teilnehmer verbundene Risiko ist immer als hoch einzuschätzen, weil diese Profile als streng vertrauliche Daten verarbeitet werden müssen.

Seq.	Art der Daten	Verarbeitet durch	Kommentar bzw. Bewertung (TMS GmbH & ext. DSB)
6.1	Lesbares Team Management Profil als PDF	TMS GmbH im Auftrag des Trainers	Versand der Team Management Profile als PDF-Anhänge per E-Mail an den Trainer
	Risiken für die Betroffenen		Vertraulichkeit, hohes Risiko Begrenzung der Speicherdauer, geringes Risiko
	Getroffene Maßnahmen		Standardmäßig wird auf alle E-Mail-Konten der TMS GmbH nur über SSL/TLS verschlüsselt zugegriffen. Weitere Sicherheitsmaßnahmen, insbesondere eine Verschlüsselung der PDF-Anhänge vor dem Versand, werden von der TMS GmbH gemäß Weisung des Trainers zur Verwendung eines bestimmten Verschlüsselungsverfahrens (z.B. PDF-Verschlüsselung mit einem vom Trainer festgelegten Passwort, ZIP-Verschlüsselung mit dem Passwort des Trainers) durchgeführt.
	Bewertung nach getroffenen Maßnahmen		Risiken beim E-Mail-Transport zum E-Mail-Server der TMS GmbH ausreichend gemindert. Für die Minderung von Risiken, z.B. im Netzwerk des Trainers, ist der Trainer (bzw. das Unternehmen des Trainers) verantwortlich.
6.2	Team Management Profil als Ausdruck	TMS GmbH im Auftrag des Trainers	Postalischer Versand an den Trainer
	Risiken für die Betroffenen		Vertraulichkeit, hohes Risiko
	Getroffene Maßnahmen		Jedes gedruckte Profil wird in einem separaten Umschlag, der mit „persönlich und vertraulich“ und dem Namen/Pseudonym des Teilnehmers gekennzeichnet ist und zudem versiegelt wird, für den Versand vorbereitet. Die entsprechend vorbereiteten Profile werden gesammelt als Paket auf den Weg gebracht.
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.
6.3	Team Management Profil als Ausdruck	TMS GmbH im Auftrag des Trainers	Postalischer Versand an den Teilnehmer
	Risiken für die Betroffenen		Vertraulichkeit, hohes Risiko

	Getroffene Maßnahmen		Das gedruckte Profil wird in einem Umschlag, der mit „persönlich und vertraulich“ gekennzeichnet ist und zudem versiegelt wird, als Brief an den Teilnehmer versendet.
	Bewertung nach getroffenen Maßnahmen		Risiken ausreichend gemindert.
6.4	Lesbares Team Management Profil als PDF	TMS GmbH im Auftrag des Trainers	Hinterlegung der Profile im Arbeitsbereich des Trainers auf profilbestellung.de (siehe Abschnitt 1 oben) für den gesicherten Download.
	Risiken für die Betroffenen		Vertraulichkeit, hohes Risiko Begrenzung der Speicherdauer, geringes Risiko
6.4.1	Lesbares Team Management Profil als PDF	TMS GmbH im Auftrag des Trainers	Hinterlegung der Profile im Arbeitsbereich des Trainers auf profilbestellung.de
	Getroffene Maßnahmen		a. Transportverschlüsselung beim Hochladen. Weitere Sicherheitsmaßnahmen, insbesondere eine Verschlüsselung der PDF-Anhänge vor dem Hochladen, werden von der TMS GmbH gemäß Weisung des Trainers zur Verwendung eines bestimmten Verschlüsselungs-verfahrens (z.B. PDF-Verschlüsselung mit einem vom Trainer festgelegten Passwort) durchgeführt. b. Die hinterlegten Profile werden automatisch 7 Tage nach Ende der Trainingsmaßnahme gelöscht. Das bietet Spielraum um im Nachgang ggf. noch auf die Profile zuzugreifen, sollte es beim Kunden Bedarf geben.
	Bewertung nach getroffenen Maßnahmen		Risiken beim Transfer in den Arbeitsbereich des Trainers sind ausreichend gemindert. Risiken bei der temporären Speicherung der druckbaren Profile auf profilbestellung.de können in Zusammenarbeit von Trainer und TMS GmbH noch deutlich gemindert werden. Eine entsprechende Sicherheitsmaßnahme, insbesondere eine Verschlüsselung der Profile vor der Hinterlegung, wird von der TMS GmbH gemäß Weisung des Trainers zur Verwendung eines bestimmten Verschlüsselungsverfahrens (z.B. PDF-Verschlüsselung mit einem vom Trainer festgelegten Passwort) durchgeführt.
6.4.2	Lesbares Team Management Profil als PDF	Trainer	Download der Profile aus dem Arbeitsbereich des Trainers auf profilbestellung.de auf ein eigenes System
	Getroffene Maßnahmen		a. Transportverschlüsselung beim Herunterladen. b. Zwei-Faktor-Authentifizierung mit temporärem Token als zweiten Faktor. 1. Der Benutzer muss sich als Faktor 1 auf Profilbestellung.de anmelden. Anmelden können sich nur akkreditierte Personen oder durch sie beauftragte Personen, die vorab von der TMS GmbH geprüft und manuell aktiviert werden. Damit soll sichergestellt werden, dass nur akkreditierte Personen und deren autorisierte Assistenzen sich im System bewegen können. Sollte es Zweifel an der Zuständigkeit einer „mutmaßlichen“ Assistenz-Person geben, wird Rücksprache mit den jeweiligen Trainern gehalten, um dieses zu verifizieren. Entsprechend verifizierte Personen können im ABS System eine Telefonnummer für den SMS Empfang des zweiten Faktors hinterlegen.

		2. Als 2. Faktor wird ein – auf Anforderung durch den Nutzer – per SMS an die hinterlegte Nummer gesendeter Code verwendet. Wird dieser Code eingegeben und stimmt die Eingabe mit dem gesendeten Code überein, werden im ABS die Download-Buttons angezeigt. Dann ist der Benutzer für ca. 10 Minuten zum Download berechtigt (temporärer Token, der nach ca. 10 Minuten gelöscht wird) und muss danach einen neuen Code anfordern. Ist ein Benutzer normal im ABS angemeldet, sieht er, dass Dateien hinterlegt sind, wird aber darauf hingewiesen, dass er eine Download-Berechtigung per SMS anfordern muss. Die Profile müssen einzeln heruntergeladen werden, der SMS Code gilt jedoch für alle für den Trainer hinterlegten Profile, bis er nach ca. 10 Minuten abläuft. Er ist also nicht für die gesamte Session gültig, sondern muss bei Zeitüberschreitung erneuert werden.
	Bewertung nach getroffenen Maßnahmen	Risiken ausreichend gemindert.

Versionskontrolle:

Version	Geändert von	Datum	Grund der Änderung	Weitergegeben an
1.0	rmn	18.06.2022	Erstellung	Frau Aurer
1.1	rmn	20.1.2022	Korrekturen in Absprache mit Aurer	
1.2	rmn	21.1.2022	Ergänzungen in Abschnitten 1 und 6.	Hr. Köpke, Fr. Aurer
1.3	rmn	5.4.2023	Insbesondere Ergänzungen in Abschnitt 6.4	Hr. Erler, Fr. Aurer
1.3.1	rmn	6.4.2023	Änderung/Korrektur nach Durchsicht durch Erler / Aurer	Als PDF an Fr. Aurer zur Veröffentlichung im Trainerbereich