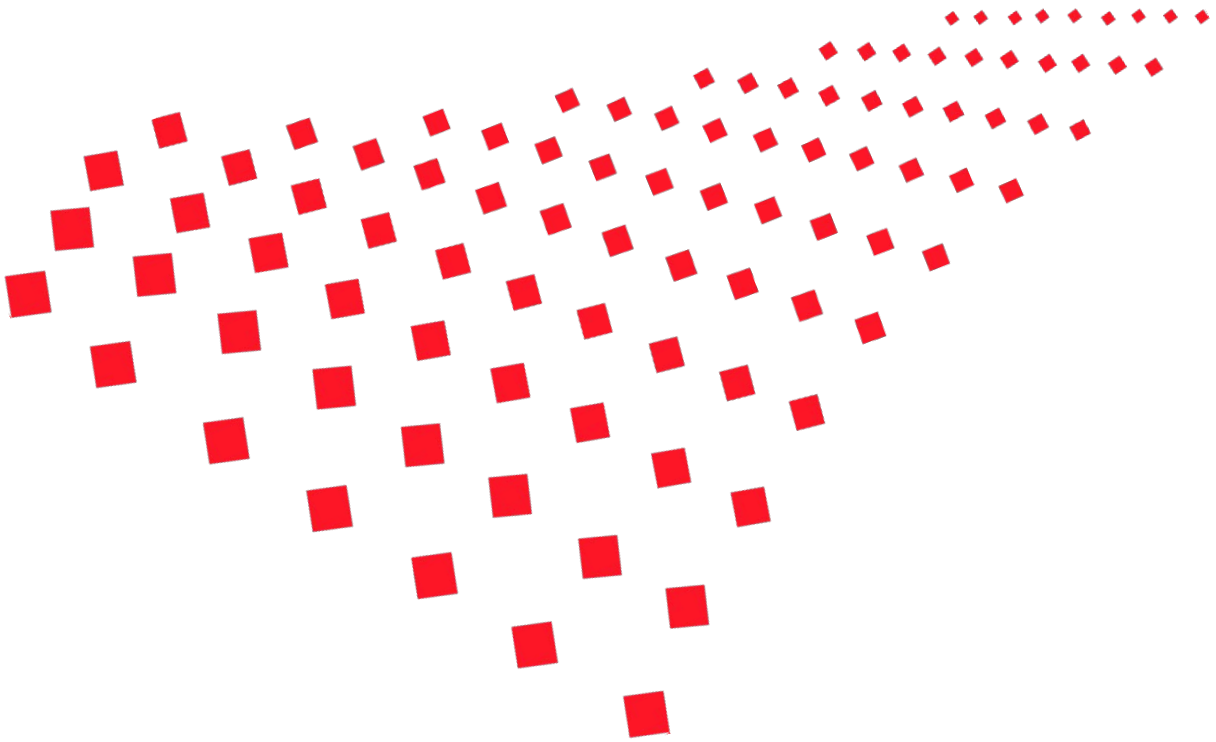
Great Place To Work.®

Datenschutz- und Datensicherheitskonzept (Stand: März 2024)



Inhaltsverzeichnis

1. Einleitung

Bei der Durchführung einer Great Place To Work® Mitarbeitendenbefragung sind Anonymität und Vertraulichkeit wichtige Voraussetzungen dafür, dass Mitarbeitende ihrem Arbeitgeber ein offenes und ehrliches Feedback geben. Datenschutz und Sicherheit haben für die GPTW Deutschland GmbH (nachfolgend „GPTW" oder Auftragnehmer genannt) höchste Priorität, und GPTW arbeitet kontinuierlich daran, ein Höchstmaß an Sicherheit und Datenschutz zu gewährleisten.

Im Folgenden wird das Konzept von GPTW zur Sicherstellung des Datenschutzes und zur Sicherung der Vertraulichkeit bzw. Anonymität der Befragungsteilnehmerinnen und Befragungsteilnehmer näher erläutert. Darüber hinaus werden in diesem Dokument auch auf die Verfahren Culture Brief™ und Culture Audit™ näher erläutert. Diese durchlaufen Unternehmen, die sich für eine Zertifizierung (Great Place To Work® Certified) und bzw. oder eine Beste Arbeitgeber Liste von Great Place To Work® bewerben. Im Gegensatz zur Great Place To Work® Mitarbeitendenbefragung werden in Culture Brief™ und Culture Audit™ keine personenbezogenen Daten verarbeitet, wohl aber vertrauliche Informationen aus dem HR-Bereich und über interne HR-Maßnahmen und Programme.

Bitte beachten Sie, dass es sich bei der Durchführung einer Great Place To Work® Befragung, bei der das Unternehmen uns Kontaktdaten der Mitarbeitenden zur Verfügung stellt, um eine Auftragsverarbeitung im Sinne von Art. 28 DSGVO handelt. In diesem Fall ist der Abschluss eines Auftragsverarbeitungsvertrags (AVV) zwischen Auftraggeber und GPTW zwingend erforderlich. GPTW stellt hierfür ein entsprechendes Vertragsmuster zur Verfügung.

2. EMRISING: SaaS-Lösung, Datenhosting und Anonymisierung der Daten

Für die Durchführung der Great Place To Work® Befragung kommt unsere flexible und innovative Befragungsplattform EMPRISING zum Einsatz. EMPRISING wird von einem unserer Partnerunternehmen – Great Place To Work® Institute, Inc. mit Sitz in Oakland, Kalifornien, USA – bereitgestellt, gewartet und weiterentwickelt. Es handelt sich hierbei um eine sogenannte „Software as a Service" (SaaS)-Lösung. Great Place To Work® Institute, Inc. fungiert demnach als Unterauftragnehmer der GPTW Deutschland GmbH. Culture Brief™ und Culture Audit™ werden über ein von Great Place To Work® Institute, Inc. entwickeltes Kundenportal abgewickelt. Das Kundenportal und die Befragungsplattform EMPRISING sind technisch miteinander verknüpft.

GPTW hat gemäß Art. 46 Abs. 2 lit. c DSGVO mit Great Place To Work® Institute, Inc. die aktuell geltenden EU-Standardvertragsklauseln (SCC) zur Auftragsverarbeitung in Drittstatten (Durchführungsbeschluss 2021/914 der EU-Kommission vom 4. Juni 2021 über EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der EU-Verordnung 2016/679 des Europäischen Parlaments und des Europäischen Rates) geschlossen (in der Processor-to-Processor-Variante gemäß Modul 3).

Zusätzlich hat GPTW, wie in der neuen Klausel 14 der SCCs mit der Überschrift "Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken" gefordert, jeweils ein Data Transfer Impact Assessment (DTIA) für Great Place To Work® Institute, Inc. (Unterauftragnehmer) und Microsoft Azure (Unterauftragnehmer seitens Great Place To Work® Institute, Inc.) durchgeführt. Kopien der SCC sowie der beiden DTIA können auf Anfrage zur Verfügung gestellt werden.

Die Datenschutz- und Sicherheitshinweise (Privacy & Security Notice) von Great Place To Work® Institute, Inc. können hier aufgerufen werden.

Als Serverstandorte kommen entweder die EU/USA (für alle Kunden, die erstmals ab dem 01.01.2024 eine Great Place To Work® Mitarbeitendenbefragung durchführen) oder die USA (für alle anderen Kunden) in Frage. In den nachfolgenden Übersichten wird die „Digital Customer Journey" für beide Varianten detailliert beschrieben.

2.1. "Digital Customer Journey" Emprising/Kundenportal (EU/US-Server)

#	Prozessschritt	Kundenportal/ Emprising	Speicherort	Anmerkung
1	Erstellung Engagement (durch GPTW)	Kundenportal	USA	- Great Place To Work® Befragung via Emprising - Culture Brief/Culture Audit© via Kundenportal
2	Bearbeitung Culture Brief™/ Culture Audit™ (durch den Kunden, kein Upload personenbezogenen Daten der Mitarbeitenden notwendig)	Kundenportal	USA	Culture Brief™: Überblick über die wichtigsten Zahlen und Fakten der Organisation Culture Audit™: Betrachtung der Personal- und Kulturarbeit der Organisation (Analyse der Prozesse, Maßnahmen und Instrumente)
3	Befragungs-vorbereitung	EMPRISING	EU (Niederlande)	Aufsetzen der Befragung (Hochladen der E-Mail-Adressen und Codes), Auswahl der Fragen
4	Befragungs-fenster	EMPRISING	EU (Niederlande)	Durchführung der Befragung (in der Regel zwei Wochen)
5	Befragungs-ergebnisse	EMPRISING	EU (Niederlande)	Darstellung der Befragungs-ergebnisse in Form von Live-Dashboards (inkl. Filter)

6	Anonymisierte Rohdaten	EMPRISING	USA & EU (Niederlande)	Die in der EU gespeicherten und anonymisierten Rohdaten werden auch in die USA übermittelt, um beispielsweise Listendaten zu extrahieren und Benchmarks zu erstellen.
7	Zertifizierung „Badge“ & Toolkit	Kundenportal	USA	

2.2. “Digital Customer Journey“ Emprising/Kundenportal (US-Server)

#	Prozessschritt	Kundenportal/ Emprising	Speicherort	Anmerkung
1	Erstellung Engagement (durch GPTW)	Kundenportal	USA	- Great Place To Work® Befragung via Emprising - Culture Brief/ Culture Audit© via Kundenportal
2	Bearbeitung Culture Brief™/ Culture Audit™ (durch den Kunden, keine personenbezogenen Daten notwendig)	Kundenportal	USA	Culture Brief™: Überblick über die wichtigsten Zahlen und Fakten der Organisation Culture Audit™: Betrachtung der Personal- und Kulturarbeit der Organisation (Analyse der Prozesse, Maßnahmen und Instrumente)
3	Befragungs-vorbereitung	EMPRISING	USA	Aufsetzen der Befragung (Hochladen der E-Mail-Adressen und Codes), Auswahl der Fragen
4	Befragungsfenster	EMPRISING	USA	Durchführung der Befragung (in der Regel zwei Wochen)
5	Befragungs-ergebnisse	EMPRISING	USA	Darstellung der Befragungsergebnisse in Form von Live-Dashboards (inkl. Filter)
6	Anonymisierte Rohdaten	EMPRISING	USA	Die in den USA gespeicherten und anonymisierten Rohdaten werden verwendet, um beispielsweise Listendaten zu extrahieren und Benchmarks zu erstellen.
7	Zertifizierung „Badge“ & Toolkit	Kundenportal	USA	

2.3. Anonymisierung der Befragungsdaten

Fünf Werktage nach Befragungsende werden die individuellen Kennungen, die zur Erfassung der Befragungsdaten verwendet wurden (in der Regel die E-Mail-Adressen der eingeladenen Befragungsteilnehmerinnen und Befragungsteilnehmer), gelöscht bzw. anonymisiert. Hierzu wird die initial gespeicherte Kennung durch eine zufällige Kennung (z.B. surveytaker1@privacy.emprising.com) ersetzt. Somit enthalten die Befragungsdaten ab diesem Zeitpunkt also weder den Namen, die E-Mail-Adresse noch irgendwelche anderen persönlichen Daten bzw. Parameter, die zur Identifizierung der Mitarbeitenden verwendet werden können.

3. Eingesetzte Unterauftragnehmer

#	**Name Unterauftragnehmer**	**Zweck der Verarbeitung**	**Kontaktdaten**
1.	Great Place To Work® Institute, Inc.*	Bereitstellung eines Kundenportals und der Befragungsplattform EMPRISING	Eingetragener Firmensitz: 1999 Harrison Street, Suite 2070 Oakland, CA 94612, USA Kontaktdaten: https://greatplacetowork.com +1 415 844 2500
Great Place To Work® Institute, Inc. setzt die folgenden Unterauftragnehmer ein:			
#	**Name Unterauftragnehmer**	**Zweck der Verarbeitung**	**Kontaktdaten**
1.1	Microsoft Azure**	Cloud-Hosting von Kundendaten, die über EMPRISING verarbeitet werden	Eingetragener Firmensitz: One Microsoft Way, Redmond, Washington 98052, USA Kontaktdaten: https://support.microsoft.com/en-us
1.2	HTEC GROUP**	Wartung der EMPRISING-Softwareplattform	Eingetragener Firmensitz: Bulevar Milutina Milankovica 11B, 11000 Belgrad, Serbien Kontaktdaten: office-bg@htecgroup.com +381 11 2281182
#	**Name Unterauftragnehmer**	**Zweck der Verarbeitung**	**Kontaktdaten**
2.	techperts GmbH*	Bereitstellung von IT-Support (IT-Service-Provider)	Eingetragener Firmensitz: Eckdorfer Straße 1, 50389 Wesseling, Deutschland Kontaktdaten: info@techperts.de +49 2236 875960

3.	Hofstede Insights Oy*	Bereitstellung einer an die Anforderungen der GPTW Deutschland GmbH angepassten Reporting-Software, sowie Bereitstellung eines Kundenportals (bspw. nutzbar zum Dateiaustausch)	Eingetragener Firmensitz: Arabiankatu 12, 00560 Helsinki, Finnland Kontaktdaten: support@hofstede-insights.com +358 923 163 043
4.	Microsoft Corporation*	Anbieter von Microsoft 365	Eingetragener Firmensitz: One Microsoft Way, Redmond, Washington 98052, USA Kontaktdaten: https://support.microsoft.com/en-us

**Unterauftragnehmer GPTW Deutschland GmbH*
***Unterauftragnehmer Great Place To Work® Institute, Inc.*

4. IT-Infrastruktur und Sicherheitsstandards der GPTW Deutschland GmbH

- Serverstandort: EU (Microsoft 365)
- Absicherung des Servers durch eine Firewall
- mehrstufiges Backup-Konzept mit logischer und räumlicher Trennung
- aktuelles, zentrales Antiviren-(AV-) und Patchmanagement
- Least-Privilege-Principle (Berechtigungs- und Rollenkonzept, Trennung von System und Daten)
- gehostete Systeme für Colloboration-Software (Exchange, SharePoint)
- Verschlüsselung nach Stand der Technik (Datenübertragung, Mobilgeräte, WLAN, VPN)
- Least-Privilege-Principle (Berechtigungs- und Rollenkonzept, Trennung von System und Daten)

5. IT-Infrastruktur und Sicherheitsstandards von Great Place To Work® Institute, Inc.

- Serverstandorte: EU/USA (für alle Kunden, die ab dem 01.01.2024 erstmalig eine Befragung über EMPRISING durchführen) oder USA (für alle anderen Kunden)
- Hosting mittels Microsoft Azure
- Absicherung des Servers durch eine Firewall
- mehrstufiges Backup-Konzept mit logischer und räumlicher Trennung
- aktuelles, zentrales Antiviren-(AV-) und Patchmanagement
- Least-Privilege-Principle (Berechtigungs- und Rollenkonzept, Trennung von System und Daten)
- Verschlüsselung „at rest“ (AES-256-Verschlüsselung) und bei der Datenübertragung (TLS 1.3) nach Stand der Technik
- Zugriff auf den Online-Fragebogen und die Live-Dashboards ausschließlich über HTTPS möglich

- Domain für die Webapplikation und Zugang zu den Live-Dashboards: https://app.emprising.com
- ISO/IEC-Zertifikate bzw. weitere Zertifikate:
  - SOC 2 Type 1
- ISO/IEC-Zertifikate bzw. weitere Zertifikate (Microsoft Azure):
  - ISO/IEC: 20000-1:2018 (Teil 1: Service-Management)
  - ISO/IEC: 22301:2019 (Business Continuity Management)
  - ISO/IEC: 27001:2013 (Informationssicherheit)
  - ISO/IEC: 27017:2015 (Informationssicherheit beim Cloud Computing)
  - ISO/IEC: 27018:2019 (Schutz persönlicher Daten in der Cloud)
  - ISO/IEC: 27701:2019 (Privacy Information Management)
  - ISO/IEC: 9001:2015 (Qualitätsmanagement)
  - CSA STAR CERTIFICATON
  - SOC 1 Type 2
  - SOC 2 Type 2
  - SOC 3

6. IT-Infrastruktur und Sicherheitsstandards von Hofstede Insights Oy

- Serverstandort: EU (Finnland)
- Serverraum entspricht dem Standard FICORA 54/2008 M der finnischen Regulierungsbehörde für Telekommunikations-dienstleistungen („Regulation on Priority Rating, Redundancy, Power Supply and Physical Protection of Communications Networks and Services“)
- Zugang zum Serverraum ist nur für ausgewählte Administratoren möglich
- Absicherung des Servers durch eine Firewall
- Verschlüsselung nach Stand der Technik (Datenübertragung, VPN)
  Zugriff auf das Kundenportal und der Download von Ergebnisberichten ausschließlich über HTTPS möglich

7. Durchführung der Great Place To Work® Befragung mittels EMPRISING

Die Administration der Befragung für den Auftraggeber erfolgt durch Projektmanagerinnen und Projektmanager bzw. Administratorinnen und Administratoren des Auftragnehmers, letztere unterstützen bei der Durchführung der Befragung. Der Unterauftragnehmer Great Place To Work® Institute, Inc. kommt lediglich ins Spiel, wenn technische Probleme auftreten, neue Features entwickelt und in Form von neuen Releases aufgespielt werden. Es besteht nur in Ausnahmefällen direkter Kontakt zwischen Auftraggeber und Great Place To Work® Institute, Inc. als Unterauftragnehmer.

Zu Projektbeginn wird für die Projektverantwortlichen des Auftraggebers ein sogenannter Administratorenzugang für das Kundenportal und EMPRISING eingerichtet. Mit diesem Zugriff können Administratorinnen bzw. Administratoren des Auftragnehmers je nach Lizenzpaket und ausschließlich für das eigene Unternehmen

Befragungen aufsetzen und starten, die Befragungsteilnahme kontrollieren, fehlerhafte E-Mail-Adressen verbessern und erneut versenden, nach Befragungsende die Befragungsergebnisse über das bereitgestellte Live-Dashboard analysieren sowie weiteren Personen (z.B. Führungskräften) Zugriff auf das Ergebnis-Dashboard gewähren. Mit dem Administratorenzugriff können darüber hinaus weitere Administratoren oder User angelegt bzw. wieder gelöscht werden. Projektmanagerinnen und Projektmanager bzw. Administratorinnen und Administratoren seitens GPTW können nach Anlegen des ersten Admin-Zugriff für eine vom Auftragnehmer genannten Person keine weiteren Admin-Zugriffe anlegen, bearbeiten oder löschen.

Die Bearbeitung des Fragebogens erfolgt ausschließlich online auf dem Server der EMPRISING-Webapplikation, wobei EMPRISING mittels Microsoft Azure gehostet wird. Der Online-Fragebogen ist für mobile Endgeräte skalierbar.

Sowohl die Webapplikation des Online-Fragebogens als auch die Übermittlung der Antwortangaben zum Umfrageserver sind hochgradig verschlüsselt (AES-256 bzw. TLS 1.3). Dies sind weltweite Sicherheitsstandards, die bspw. beim Online-Banking zum Einsatz kommen, damit kritische Kundendaten sicher sind.

Befragungsergebnisse können während der Befragung nicht eingesehen werden, sondern ausschließlich Rücklaufübersichten. Nach dem Abschluss der Befragung kann die Administratorin bzw. der Administrator in EMPRISING nur die aggregierten bzw. aufbereiteten Befragungsergebnisse einsehen. Ein Zugriff auf Antworten individueller Befragungsteilnehmerinnen und Befragungsteilnehmer ist zu keinem Zeitpunkt möglich, da dies technisch innerhalb von EMPRISING nicht möglich ist (Privacy by Design).

7.1. Online-Befragung mittels E-Mail-Link

Zu Beginn der Befragung werden die Mitarbeitenden per E-Mail zur Teilnahme an der Befragung eingeladen. Die Einladungs-E-Mails enthalten jeweils einen personalisierten Link, d.h. eine eindeutige Anmeldekennung, über den die eingeladenen Mitarbeitenden zum Fragebogen gelangen. Das Unternehmen bzw. die einladenden Mitarbeitenden müssen sicherstellen, dass die individuellen Einladungs-E-Mails nicht innerhalb des Unternehmens oder an Dritte weitergegeben werden.

7.2. Online-Befragung mittels Code(brief)

Bei einer Befragung mit Code(brief) wird keine E-Mail-Adresse benötigt, stattdessen können sich die eingeladenen Mitarbeitenden mit einem individuellen Befragungscode einloggen. Um die Befragung starten zu können, muss der Auftraggeber sicherstellen, dass die individuellen Zugangscodes an alle eingeladenen Mitarbeitenden verteilt werden. Darüber hinaus erhalten die Mitarbeitenden einen Login-Link zur Online-Fragebogen. Dieser wird für jede Befragung neu erstellt.

Beim Versand der Zugangscodes ist darauf zu achten, dass Codes nicht Dritten und vor allem nicht Führungskräften oder anderen Mitarbeitenden offengelegt werden, da ansonsten eine anonyme Teilnahme nicht mehr gewährleistet werden kann. Die Vergabe und der Versand der Zugangscodes kann optional von GPTW übernommen werden (auf Anfrage und gegen Aufpreis).

7.3. Vorbereitung der Mitarbeitendenbefragung

Ein wesentlicher Bestandteil innerhalb der EMPRISING-Webapplikation ist das Hochladen einer Datei mit Mitarbeitendendaten (*Employee Data File*, kurz: EDF). Die EDF enthält entweder eine Liste der E-Mail-Adressen oder eine Liste der selbst generierten Zugangscodes. Optional kann die EDF noch weitere demografische Merkmale (z.B. organisatorische Zuordnung, hierarchische Ebene etc.) enthalten. Das Unternehmen erstellt die EDF mit Hilfe der Anweisungen innerhalb von EMPRISING selbst.

Für die volle Sicherstellung der Vertraulichkeit der Befragungsteilnehmer ist es erforderlich, bestimmte Standards bei der Erstellung der EDF einzuhalten. Ein entsprechendes Merkblatt ist im Vertragsmuster enthalten (vgl. Anlage 1 Muster-AV-Vertrag).

8. Auswertung der Great Place To Work® Mitarbeitendenbefragung

Die Great Place To Work® Befragung enthält:

- geschlossene Fragen, hier konkret Bewertungen zu Aussagen wie „Die Mitarbeitenden werden hier angemessen bezahlt.“ anhand mehrerer, vordefinierter Antwortkategorien auf Grundlage einer fünfstufigen Likert-Skala (Antwortkategorien: „trifft fast gar nicht zu“, „trifft überwiegend nicht zu“, „teils/teils", „trifft überwiegend zu“ und „trifft fast völlig zu“),
- offene Fragen mit sog. Freitextfeldern, in die Befragungsteilnehmerinnen und Befragungsteilnehmer eine beliebige Antwort eingeben können,
- Fragen zu (sozio-)demografischen Merkmalen wie bspw. Altersgruppe, Art der Beschäftigung, berufliche Position usw.

Sowohl die Teilnahme an der Befragung selbst wie auch die Beantwortung jeder einzelnen Frage im Fragebogen ist **freiwillig**. Die Auswertungen erfolgen ausschließlich auf Grundlage von anonymisierten Datensätzen („Rohdaten“), die keinerlei individuelle Kennungen wie bspw. E-Mail-Adressen enthalten (siehe Kapitel „2.3. Anonymisierung der Befragungsdaten“).

Befragungsergebnisse werden innerhalb von EMPRISING in einem Ergebnis-Dashboard angezeigt bzw. können in Form eines tabellarischen Ergebnisberichts von den Administratorinnen bzw. Administratoren des Auftragnehmers heruntergeladen werden.

Die finalen Befragungsergebnisse aller geschlossenen und demografischen Fragen werden bei sämtlichen Auswertungen und Ergebnisberichten ausschließlich in aggregierter Form dargestellt. Zusätzlich wird eine Auswertungsgrenze – d.h. eine Mindestanzahl von Antwortenden – festgelegt, unterhalb derer keine Ergebnisse in den Ergebnis-Dashboards bzw. in den Berichten dargestellt werden. Als Standardwert ist eine Auswertungsgrenze von fünf Antworten definiert. Dies gilt auch dann, wenn die Administratorin bzw. der Administrator Ergebnisse für bestimmte Teilgruppen (z.B. alle Frauen) einsieht. Auch Kombinationen von bis zu drei Gruppen (z.B. alle Frauen in einer bestimmten Altersgruppe und auf einer bestimmten Führungsebene) sind prinzipiell möglich. Auch hier werden Ergebnisse wiederum nur angezeigt, wenn bei der Kombination der Gruppen mindestens fünf Teilnehmende übrigbleiben.

Einschränkend ist festzustellen, dass es durch Negativselektion im Einzelfall nicht ausgeschlossen werden kann, dass Rückschlüsse auf die Antworten einzelner Personen vorgenommen werden. Entsprechende Rückschlüsse sind immer Vermutungen, da den Auswerterinnen und Auswertern niemals bekannt gemacht wird, welche Personen tatsächlich an der Befragung teilgenommen haben. Das Risiko einer Negativselektion lässt sich vor allem dadurch minimieren, dass nur einem eingeschränkten Personenkreis Zugriff auf die Ergebnis-Dashboards gegeben wird, die Auswertungsmöglichkeiten für Führungskräfte, die Ergebnisse ihres Verantwortungsbereich einsehen können, und bei demografischen Merkmalen, die mit dem EDF hochgeladen werden, kleine Gruppe zu vermeiden (vgl. Anlage 1 Muster-AV-Vertrag).

Antworten auf offene Fragen werden standardmäßig im „Original-Ton", d.h. in der Originalsprache und ohne entsprechende Anonymisierung von Namen oder sonstigen Hinweisen, die Rückschlüsse auf einzelne Personen zulassen, dargestellt bzw. berichtet. Darüber hinaus empfehlen wir, den Sachverhalt im Vorfeld der Befragung an alle Mitarbeitenden zu kommunizieren. Im Zuge dessen sollten Mitarbeitende angewiesen werden, keine Namen zu nennen bzw. Sachverhalte derart zu schildern, so dass keine Rückschlüsse auf sie selbst oder auf einzelne Personen möglich sind.

Eine Zuordnung der Antworten auf die offenen Fragen zu einzelnen Organisationseinheiten bzw. zu den Angaben zu den demografischen Fragen ist nur möglich, wenn in einer Organisationseinheit bzw. in einer demographischen Gruppe standardmäßig mindestens fünf Personen an der Befragung teilgenommen haben.

GPTW stellt keine „Rohdaten" zur Verfügung, mit denen der Auftraggeber eigene Auswertungen vornehmen kann.

Anonymisierte Befragungsdaten aus der Great Place to Work® Befragung können für Vergleichsanalysen und Veröffentlichungen durch GPTW Deutschland, durch Partnerorganisationen im weltweiten GPTW-Netzwerk sowie im Rahmen von Forschungskooperationen mit Universitäten und anderen Forschungseinrichtungen genutzt und

verarbeitet werden. Darüber hinaus speichert GPTW dauerhaft anonymisierte Rohdaten in einer firmeneigenen Datenbank, um diese für kundenindividuelle sowie unternehmensübergreifende Auswertungen und Berichte nutzen zu können. Bei sämtlichen Auswertungen und Berichten werden die in den Allgemeinen Geschäftsbedingungen der GPTW Deutschland GmbH festlegten Standards zur Vertraulichkeit der Befragungsergebnisse jedes einzelnen Auftraggebers eingehalten.

9. Das Great Place to Work® Culture Brief™ und Culture Audit™

Das Great Place to Work® Culture Audit™ bzw. Culture Brief ™ ist eine Befragung zu Maßnahmen und Programmen im HR-Bereich und zu Statistiken über die Mitarbeitendenstruktur (z.B. Anzahl männliche und weibliche Mitarbeitende, Anzahl Mitarbeitende auf verschiedenen Hierarchieebenen). Neben entsprechenden Angaben werden die Unternehmen gebeten, Fotos von ihren Arbeitsplätzen und von Mitarbeitenden bei der Arbeit einzureichen.

Unternehmen erhalten über das Culture Audit ™ eine Rückmeldung zur Qualität ihrer Maßnahmen und Programme im Vergleich zu sehr guten Arbeitgebern. Darüber hinaus ist das Culture Audit™ neben den Ergebnissen der Great Place To Work® Befragung ein zentrales Bewertungskriterium im Rahmen des Wettbewerbs „Deutschlands Beste Arbeitgeber“ und der angeschlossenen Regional- und Branchenwettbewerbe. Das Culture Brief ist eine Voraussetzung für eine erfolgreiche Zertifizierung Great Place To Work® Certified.

Für die Bearbeitung von Culture Brief™ und Culture Audit™ sind keine weiteren personenbezogene Daten relevant. Die Fragebögen werden von denen im Kundenportal angelegten Administratorinnen und Administratoren bearbeitet.

Ansonsten enthalten Culture Brief™ und Culture Audit™ keine personenbezogenen Daten – es sei denn, ein Unternehmen entscheidet sich dazu, im Culture Audit™ Namen einzelner Mitarbeitenden zu nennen bzw. Fotos von Mitarbeitenden einzureichen.

Culture Brief™ und Culture Audit™ werden im Rahmen eines Online-Fragebogens durchgeführt. Hierbei macht das teilnehmende Unternehmen statistische Angaben und stellt eigene Maßnahmen und Programme textlich dar. Ferner gibt es die Möglichkeit, im Online-Fragebogen Materialien hochzuladen und diese mit GPTW zu teilen. Daten aus dem Great Place To Work® Culture Audit™ können für Vergleichsanalysen und Veröffentlichungen durch GPTW, durch Partnerorganisationen im weltweiten GPTW-Netzwerk und im Rahmen von Forschungskooperationen mit Universitäten und anderen Forschungseinrichtungen genutzt und verarbeitet werden. Dabei bleibt die Vertraulichkeit der Information jederzeit gewahrt. Eine Veröffentlichung von Informationen aus dem Culture Audit™, die auf ein spezifisches Unternehmen rückführbar sind, erfolgt nur nach ausdrücklicher Einwilligung des betroffenen Unternehmens.

10. Technische und organisatorische Maßnahmen der GPTW Deutschland GmbH

Vorwort
Die GPTW Deutschland GmbH legt großen Wert auf einen bestmöglichen Schutz personenbezogener Daten. Daher gibt es umfangreiche technische und organisatorische Maßnahmen, um ein hohes Schutzniveau zu erreichen. Das Dokument beschreibt daher die als verbindlich festgelegten technischen und organisatorischen Maßnahmen im Zusammenhang mit durchgeführten Auftragsverarbeitungsvorgängen zwischen Auftraggeber und Auftragnehmer. Die dargestellten Maßnahmen stellen somit ein Abbild des gelebten Datenschutz- und Datensicherheitskonzept des Auftragnehmers dar.

Allgemeines
Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Auftragsverarbeitung getroffenen technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs.1 DSGVO.

Die DSGVO verpflichtet Unternehmen die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu anonymisieren oder zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen. Diese Anforderungen erfüllt der Auftragnehmer durch angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
Zutrittskontrolle

(Es sind Maßnahmen zu treffen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)

Gebäudeart
Bei dem genutzten Gebäude handelt es sich im Wesentlichen um ein Bürogebäude mit vier Stockwerken und einem nutzbaren Keller, welches vorrangig von der GPTW Deutschland GmbH genutzt wird.

Im Erdgeschoss befindet sich eine Kindertagesstätte. Die Verbindungstüre zwischen der Kindertagesstätte und den Büroräumlichkeiten beziehungsweise dem Treppenhaus von GPTW Deutschland GmbH ist stets verschlossen.

Das Gebäude befindet sich innerhalb eines Betriebsgeländes. Das Betriebsgelände, die Gebäudeaußenwände und die Fenster wurden bei den Zutrittskontrollmaßnahmen berücksichtigt.

Das Betriebsgelände und somit auch das Betriebsgebäude sind umzäunt, beziehungsweise ummauert und von außen gut beleuchtet.

Der Haupteingang ist durch ein Sicherheitsschloss gesichert. Es existieren weder Hinternoch Nebeneingänge oder Lichtschächte und Lüftungsöffnungen. Die Fenster bestehen aus Isolierverglasung. Sowohl der Aufzug als auch das Treppenhaus sind ebenfalls in das Sicherheitssystem einbezogen. Um das Treppenhaus oder den Aufzug betreten zu können, müssen Besucher klingeln und werden mittels Gegensprechanlage mit Kamera durch Mitarbeitende des Sekretariats identifiziert und anschließend Einlass gewährt.

Die einzelnen Etagen werden nach Arbeitsende verschlossen.

Zutritt ausreichend gesichert
Durch die Identifizierung von Besuchern durch Mitarbeitende des Sekretariats ist gewährleistet, dass sich Besucher zwangsläufig anmelden müssen und nicht unbefugt in das Gebäude gelangen können.

Zutrittsberechtigungen
Auf den einzelnen Büroetagen erfolgt eine Trennung von Bearbeitungs- und Publikumszonen.

Vor Feierabend werden die Räumlichkeiten überprüft, um zu verhindern, dass Unbefugte einschließen lassen.

Schlüsselregelungen
Sämtliche Schlüssel sind in einem Schlüsselregister erfasst. Die Ausgabe und Rücknahme von Schlüsseln werden entsprechend dokumentiert und quittiert. Überzählige Schlüssel werden in ausreichend sicher gestalteten Schlüsselkästen verwahrt, auf welche nur die Mitarbeitende des Sekretariats Zugriff haben.

Die Schlüssel sind der Art, dass diese nicht einfach unbefugt dupliziert werden können. Sollte ein Schlüssel von einer/einem ausgeschiedenen Mitarbeitende/n nicht zurückgegebenen werden, so werden die Schlösser ausgetauscht. Gleiches gilt bei Verlust eines Schlüssels.

Zutrittskontrollierte Zonen
Alle Datenverarbeitungsanlagen, mit denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, befinden sich in zutrittskontrollierten Zonen.

Für den Fall, dass externe Kräfte Zutritt benötigen (z.B. Wartungsdienste, Reinigungsdienste, Besucher), müssen sich die externen Kräfte zunächst den üblichen Zutrittskontrollprüfungen unterziehen und dürfen sich danach nur im Rahmen ihrer vorher festgelegten Privilegien bewegen.

Die Server/Firewalls sind in einem abgeschlossenen, fensterlosen Raum (Serverraum) installiert, der mittels einer verschlossenen Stahltür gesichert ist. Zusätzlich sind die Server in speziellen Serverschränken verschlossen. Durch entsprechende interne Maßnahmen ist sichergestellt, dass nur berechtigte Personen Zutritt zum Serverraum erhalten.

Die Verteilerräume (Strom, Wasser, Fernwärme, Telefon) sind ebenfalls gegen unbefugten Zutritt gesichert. Auch durch die An- und Ablieferung von Datenträgern, Belegen, Listen usw. wird das Sicherheitssystem nicht durchbrochen.

Die Aufbewahrungsorte für mobile Endgeräte (wie Notebooks) wurden bei den Zutrittskontrollmaßnahmen berücksichtigt.

Gebäudereinigung
Die Gebäudereinigung wird durch ein externes Unternehmen durchgeführt.

Telearbeit und Heimarbeit („Homeoffice")
Es findet Heimarbeit statt, es sei denn, diese wird durch einen Auftraggeber vertraglich ausgeschlossen.

Zugangskontrolle
(Es sind Maßnahmen zu treffen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)

Zugang
Für die Zugangskontrolle existiert ein Sicherheitskonzept.

Die Server/Firewalls sind in einem abgeschlossenen, fensterlosen Raum (Serverraum) installiert, der mittels einer verschlossenen Stahltür gesichert ist. Zusätzlich sind die Server in speziellen Serverschränken verschlossen. Durch entsprechende interne Maßnahmen ist sichergestellt, dass nur berechtigte Personen Zutritt zum Serverraum erhalten.

Endgeräte sind mittels Passwortschutz gegen unbefugte Benutzung gesichert.

Netzwerk
Jeder DV-Benutzer verfügt über eine eigene Benutzerkennung (User-ID) zuzüglich eines Passworts, ohne die eine Anmeldung am System nicht möglich ist.

Es besteht die Möglichkeit, der Softwareverriegelung der Bildschirme, so dass eine Weiterarbeit erst nach Eingabe eines Passworts möglich ist. Der Bildschirmschoner aktiviert sich 10 Minuten nach der letzten Benutzereingabe automatisch. Daneben gibt es die Anweisung, die Endgeräte oder Personal Computer nach Beendigung der Arbeit beziehungsweise beim Verlassen des Arbeitsplatzes herunterzufahren oder

gegen unbefugte Benutzung zu sperren.

Es erfolgt eine Abschottung des internen Netzes gegen ungewollte Zugänge von außen mithilfe einer Firewall.

Passwörter

Es gibt schriftlich dokumentierte Regeln für sichere Passwörter, die durch eine Passwortrichtlinie erzwungen werden: Die Mindestlänge des Passworts beträgt acht Zeichen, zudem müssen Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern enthalten sein. Das Passwort muss nach 42 Tagen erneuert werden und darf sich frühestens nach drei Änderungen wiederholen. Die fehlerhafte Eingabe eines Kennwortes führt nach fünf Fehlversuchen zur Sperrung des bezogenen Benutzerkontos. Benutzerkonten, die länger als 90 Tage nicht in Benutzung sind, sind zu sperren.

Es werden nur Individualpasswörter vergeben, keine Gruppenpasswörter.

Bei der ersten Anmeldung muss der Benutzer das vom Administrator vorgegebene Passwort ändern. Zudem werden die Passwörter verschlüsselt gespeichert und somit ist ein Zugriff unbefugter Dritter ausgeschlossen. Der Auftragnehmer hat IT-Leit- und Richtlinien entwickelt, welche an alle Beschäftigten der GPTW Deutschland GmbH verteilt wurde. Neuen Mitarbeitenden wird diese Richtline zu Beginn des Beschäftigungsverhältnisses ausgehängt. Ein wichtiger Punkt dieser Leitlinie sind die Regeln für einen sicheren und datenschutzkonformen Passwortgebrauch.

Bei Pausen oder längerer Abwesenheit (ab 10 Minuten) aktiviert sich die Bildschirmsperre mit Passwortaktivierung automatisch.

Es wird das „Single sign on“ (SSO)-Verfahren eingesetzt, so dass der Benutzer mit einmaliger Authentifizierung am Arbeitsplatz Zugriff auf alle Rechner und Dienste erhält, für die er lokal berechtigt ist. Die sichere Übertragung der Passwörter im Netz erfolgt mittels des Netzwerkprotokolls „Kerberos“. Dieser Dienst authentifiziert sowohl den Server gegenüber dem Client, als auch den Client gegenüber dem Server. Auch der Kerberos- Server selbst authentifiziert sich gegenüber dem Client und dem Server und verifiziert selbst deren Identität. Zudem werden die Passwörter verschlüsselt gespeichert und somit ist ein Zugriff unbefugter Dritter ausgeschlossen.

Die Default-Passwörter aller relevanten Systeme sind deaktiviert.

Zugangsberechtigungen

Zugangsberechtigungen (Benutzerkennung und Passwort) einer/eines ausgeschiedenen Mitarbeitende/n werden sofort gesperrt. Die Verwaltung und Pflege der Zugangs-berechtigungen sind eindeutig geregelt.

„Unterwegs“ befindliche Datenträger/Festplatten werden nach Stand der Technik verschlüsselt.

Sensible Papierunterlagen werden in einwandigen Stahlschränken verwahrt.

Firewall
Es werden sowohl eine Hardware-Firewall als auch eine Software-Firewall eingesetzt. Updates der Hardware-Firewall werden durch den externen IT-Dienstleister manuell installiert, Updates der Software-Firewall automatisch bei Erscheinen.

Browser
Die genutzten Browser sind der Microsoft Edge, Mozilla Firefox sowie Google Chrome. Sicherheitsupdates/Patches werden laufend in einem automatisierten Verfahren installiert.

Systemadministration
Die Systemadministration ist im Rahmen einer Datenverarbeitung im Auftrag gemäß den Anforderungen nach Art. 28 DSGVO an die techperts GmbH, Eckdorfer Straße 1 in 50389 Wesseling ausgelagert.

Die Administratoren verfügen über getrennte Benutzerkonten für Systemadministration und Sachbearbeitung. Die Administrationsarbeit wird protokolliert. Die Protokolle werden anlassbezogen ausgewertet.

Zugriffskontrolle
(Es sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, 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.)

Allgemeiner Schutz
Sensible Daten sind gegen zufälligen unbefugten Einblick mittels blickdichter Türen geschützt.

Das Unternehmen schützt sich gegen Malware und unbefugte Zugriffe von außen. Dies geschieht mittels Antivirensoftware, einer Hardware-Firewall sowie einer Software-Firewall. Updates der Hardware-Firewall werden durch den externen IT- Dienstleister manuell installiert, Updates der Antivirensoftware und der Software- Firewall automatisch bei Erscheinen.

Es werden Verschlüsselungsverfahren nach Stand der Technik eingesetzt, bis diese nachweislich kompromittiert sind oder verbesserte Varianten vorliegen.

Datenverarbeitungssystem(e) (DV-Systeme)
Für die Benutzung der DV-Systeme mit denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden müssen Benutzerkennungen eingegeben werden. Diese werden durch den externen IT-Dienstleister eingerichtet. Diesbezüglich existieren Richtlinien für die Vergabe der Benutzerkennungen. Dadurch ist gewährleistet, dass jeder Benutzer nur auf diejenigen Dienste zugreifen kann, die zur Erfüllung der Aufgaben benötigt werden.

Es werden bei der Umfrage ausschließlich Daten erhoben, die einerseits für den Verarbeitungszweck erforderlich sind (Datensparsamkeit) und andererseits mit dem Verantwortlichen abgestimmt wurden, um möglichst wenig in die Schutzrechte der freiwilligen Teilnehmer von Umfragen einzugreifen. Datenbankfelder werden pseudonymisiert bzw. anonymisiert, sobald die eingegebenen Echtdaten nicht mehr unbedingt erforderlich sind. Daneben greift ein Löschkonzept (Datenvermeidung und -minimierung).

Sämtliche genutzte Webdienste sind datenschutzfreundlich voreingestellt, Daten werden nach Stand der Technik verschlüsselt übertragen und gespeichert.

Berechtigungen erfolgen jeweils auf einem standardisierten Weg und somit nicht auf „Zuruf".

Die DV-Systeme unterstützen eine Zugriffssicherung durch Verstecken, Schreibschützen, Verschlüsseln sowie Sperren von Dateien und Verzeichnissen. Eine Beschränkung der Anmeldezeiten ist möglich.

Passwörter
Es gibt schriftlich dokumentierte Regeln für sichere Passwörter, die durch eine Passwortrichtlinie erzwungen werden: Die Mindestlänge des Passworts beträgt acht Zeichen, zudem müssen Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern enthalten sein. Das Passwort muss nach 42 Tagen erneuert werden und darf sich frühestens nach drei Änderungen wiederholen. Die fehlerhafte Eingabe eines Kennwortes führt nach fünf Fehlversuchen zur Sperrung des bezogenen Benutzerkontos. Benutzerkonten, die länger als 90 Tage nicht in Benutzung sind, werden gesperrt.

Es werden nur Individualpasswörter vergeben, keine Gruppenpasswörter.

Bei der ersten Anmeldung muss der Benutzer das vom Administrator vorgegebene Passwort ändern. Zudem werden die Passwörter verschlüsselt gespeichert und somit ist ein Zugriff unbefugter Dritter ausgeschlossen. Der Auftragnehmer hat IT-Leit- und Richtlinien entwickelt, welche an alle Beschäftigten der GPTW Deutschland GmbH verteilt wurde. Neuen Mitarbeitenden wird diese Richtline zu Beginn des Beschäftigungsverhältnisses ausgehängt. Ein wichtiger Punkt dieser Leitlinie sind die Regeln für einen sicheren und datenschutzkonformen Passwortgebrauch.

Bei Pausen oder längerer Abwesenheit (ab 10 Minuten) aktiviert sich die Bildschirmsperre mit Passwortaktivierung automatisch.

Es wird das „Single sign on"-Verfahren eingesetzt, so dass der Benutzer mit einmaliger Authentifizierung am Arbeitsplatz Zugriff auf alle Rechner und Dienste erhält, für die er lokal berechtigt ist. Die sichere Übertragung der Passwörter im Netz erfolgt mittels des Netzwerkprotokolls „Kerberos". Dieser Dienst authentifiziert sowohl den Server gegenüber dem Client, als auch den Client gegenüber dem Server. Auch der Kerberos-Server selbst authentifiziert sich gegenüber dem Client und dem Server und verifiziert selbst deren Identität.

Zudem werden die Passwörter verschlüsselt gespeichert und somit ist ein Zugriff unbefugter Dritter ausgeschlossen.

Die Default-Passwörter aller relevanten Systeme sind deaktiviert.

Netzwerke und Server
Für den Zugriff auf das Netzwerk ist die Eingabe einer Benutzerkennung und eines Passworts erforderlich.

Die Rechtevergabe erfolgt benutzerspezifisch abgestuft auf Verzeichnis- und Dateiebene. Die Betriebssystemebene ist für den normalen Anwender gesperrt. Die Speicherung von Daten auf lokalen Arbeitsplatzrechnern und eben nicht auf dem gut geschützten Server ist untersagt.

Es werden für die Auswertung aller (unberechtigten) Dateizugriffe Protokolle geführt. Diese werden anlassbezogen ausgewertet.

Fehlerdiagnose/Fernwartung
Es werden ausreichende Sicherheitsmaßnahmen für die Fehlerdiagnose, Wartung und Fernwartung ergriffen, so dass erkennbar ist, wer wann worauf zugegriffen hat.

Für die Fernwartung/Ferneinwahl werden Protokolle geführt. Diese werden anlassbezogen ausgewertet.

Der Zugriff per Fernwartung erfolgt ausschließlich durch betriebliche Computer, die über den gleichen Sicherheitsstandard verfügen wie lokale, betriebliche PCs. Bei der lokalen Wartung durch Externe ist sichergestellt, dass kein Equipment (z.B. Geräte oder Datenträger) den DV-Bereich unkontrolliert verlassen kann.

Notebooks und Smartphones
Es existiert eine Richtlinie für den Umgang mit mobilen Endgeräten wie Notebooks oder Smartphones.

Papierhafte Unterlagen und Office-Dokumente
Der Zugriff auf papierhafte Unterlagen/Akten wird geschützt. Sensible Akten werden im Sekretariat verschlossen aufbewahrt.

Es wird der Grundsatz des aufgeräumten Schreibtischs („Clean Desk“) und des leeren Bildschirms gelebt, so dass weder in Papierform vorhandene noch auf Datenträgern abgelegte personenbezogene Informationen längere Zeit auf dem Schreibtisch des Nutzers verbleiben.

Zu vernichtende Papierunterlagen/Akten werden in einem verschließbaren Sammelcontainer aufbewahrt und nach Bedarf durch einen zertifizierten Dienstleister vernichtet.

Sensible Daten bzw. Dokumente mit personenbezogenen Daten werden vor Manipulation und gegen Einblicke unbefugter Dritter geschützt, indem sie nach Stand der Technik verschlüsselt werden, so dass nur berechtigte Personen darauf Zugriff erhalten.

Löschung von Daten
Zu vernichtende Unterlagen und Datenträger werden durch ein zertifiziertes und schriftlich auf Art. 28 DSGVO verpflichtetes Entsorgungsunternehmen datenschutzkonform entsorgt. Die Übergabe wird protokolliert.

Löschungen (in Form von mehrfachem Überschreiben) von Daten vor Ort werden in einer Protokolldatei dokumentiert. Die Löschfristen sind in der internen Verarbeitungsübersicht beziehungsweise im Verfahrensverzeichnis definiert, so dass sichergestellt ist, dass Löschfristen eingehalten werden. Mitarbeitende sind über die Aufbewahrungs- und Löschfristen demgemäß informiert.

Datensicherungen sind verschlüsselt. Durch die Vernichtung des jeweiligen Kennwortes wird somit indirekt die Löschung der Datensicherung ermöglicht.

Ausgestaltung des Berechtigungskonzeptes und der Zugriffsrechte
Es gibt eine Organisationsrichtlinie, welche vorschreibt, dass neu einzurichtende Berechtigungen, Berechtigungsänderungen oder Berechtigungslöschungen immer in Textform angefordert werden müssen. Daneben existieren ein programmtechnisches Berechtigungskonzept (differenzierte Berechtigungen für Daten und Betriebssystem) und ein Rollenkonzept mit Rollendefinition.

Protokollierung
Eine Verfahrensanweisung regelt die Art und den Umfang der Protokollierung. Es werden sämtliche Dateizugriffe mittels des Domaincontrollers protokolliert (sowohl „success“ als auch „fail“, hierbei ist standardmäßig ein volles „security logging“ aktiviert). Die gespeicherten Protokolle werden bei Bedarf durch den externen IT-

Dienstleister ausgewertet. Eine Löschung der gespeicherten Protokolle findet durch „rollierende Überschreibung“ statt.

Datenträger
Verantwortlich für die Datenträger ist das Sekretariat. In einer Verfahrensanweisung/ Richtlinie ist geregelt, welche Personen befugt sind, Datenträger zu entnehmen.

Verwendete Datenträger werden nach Stand der Technik verschlüsselt. Die verschlüsselten Datensicherungsträger sind in eine andere Brandschutzzone ausgelagert.

Datenträgerverwaltung
Es werden Nachweise über den Eingang, den Ausgang sowie den Bestand von Datenträgern durch den Empfang geführt. Ausgabe, Weitergabe und Rücknahme von Datenträgern erfolgt gegen Quittung. Daneben erfolgt, ebenfalls durch den Empfang, eine Protokollierung bei Aussonderung von Datenträgern. Auch werden regelmäßig Datenträgerinventuren durchgeführt. Benutzte Datenträger werden zugriffssicher aufbewahrt.

Der Einsatz privater Datenträger ist strikt verboten.

Datenträgervernichtung und Datenträgerentsorgung
Es existiert eine Richtlinie welche regelt, wie Fehldrucke entsorgt/vernichtet werden.

Nicht mehr benötigte und/oder defekte Datenträger werden mittels Einsatzes eines geeigneten und auf Art. 28 DSGVO verpflichteten Entsorgungsunternehmen datenschutzkonform vernichtet und entsorgt. Das Vorgehen für den Fall, dass ein nicht löschbarer Datenträger mit personenbezogenen Daten wegen Unbrauchbarkeit oder aus sonstigen Gründen (z.B. Vernichtung) weitergegeben wird, ist ebenfalls geregelt. Der Datenträger wird in einem Stahlschrank im Serverraum zwischengelagert und anschließend an das Entsorgungsunternehmen ausgehändigt. Zur Löschung vorgesehene Datenträger werden ebenfalls sicher in einem Stahlschrank im Serverraum zwischengelagert.

Zugriffsschutz durch Bildschirmschoner
Bei Pausen oder längerer Abwesenheit (ab 10 Minuten) aktiviert sich die Bildschirmsperre mit Passwortaktivierung automatisch.

Trennungsgebot
(Es sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)

Richtlinien
Es gibt ein schriftliches Konzept für die Datenerhebung und Datenverarbeitung. Das Konzept beinhaltet Regelungen und Maßnahmen zur Sicherung der getrennten

Speicherung, Veränderung, Löschung und Übermittlung von Daten mit unterschiedlichen Vertragszwecken. Ferner gibt es technische und organisatorische Kontrollmaßnahmen zur Sicherstellung der Zweckbindung.

Datenbanken
Datenbankbenutzer sind in der Verwendung der Datenbank geschult. Die Zugriffsrechte von Datenbanknutzern sind auf das Notwendigste reduziert, um die Integrität der Daten bestmöglich zu gewährleisten. Daten verschiedener Auftraggeber werden dabei so gespeichert, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Gespeicherten Daten des Auftraggebers sind logisch von gespeicherten Daten anderer Auftraggeber getrennt (Mandantentrennung).

Ein schriftliches Konzept beschreibt, wie Daten für Testzwecke gewonnen werden und wie damit umzugehen ist. Dadurch ist sichergestellt, dass im Entwicklungs- und Testsystem nur Testdaten verarbeitet werden. Auch ist sichergestellt, dass Testdaten, die aus Echtdaten abgeleitet werden sollen, anonymisiert sind.

Zugriffe über Anwendungen werden nur nach Erfordernis eingerichtet. Es gibt klare Regelungen für die Archivierung.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)
Weitergabekontrolle
(Es sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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.)

Datenträgertransporte
Es finden lediglich Datenträgertransporte zwecks Auslagerung der Sicherungsdatenträger an den externen IT-Dienstleister statt. Diese Datenträger sind stets verschlüsselt.

Arten der Datenübertragung
Der Datenversand/die Datenübertragung erfolgt per Briefpost, E-Mail, Telefax, IP-Telefonie, Internet, sFTP sowie HTTPS. Bei der digitalen Telefonie via VoIP kommen die Programme Placetel, Zoiper, Zoom sowie MS Teams zum Einsatz.

Grundsätzlich werden bei der Übertragung (primäre Leitung: Kabelanschluss sowie sekundäre Leitung: SHDSL) Verschlüsselungsverfahren nach Stand der Technik eingesetzt. Es werden stets Punkt-zu-Punkt-Verschlüsselungen nach Stand der Technik eingesetzt.

Sofern ein öffentliches Netzwerk wie beispielsweise ein öffentliches W-LAN-Hotspot

außerhalb des Firmengebäudes genutzt wird, erzwingt eine Gruppenrichtlinie restriktive Einstellungen auf Betriebssystemebene.

Transportsicherung
Sofern ein Datenträgertransport stattfindet, werden verschließbare Transportbehälter benutzt, so dass ein Schutz gegen unbefugten Zugriff und Beschädigung sichergestellt ist. Vor dem Transport werden Sicherheitskopien angelegt, um die Daten vor zufälligem Verlust oder zufälliger Zerstörung zu schützen. Zusätzlich werden zu transportierende Datenträger nach Stand der Technik geschützt (AES-256-Verschlüsselung).

Transportunternehmen werden auf Zuverlässigkeit und Sicherheit überprüft. Zudem sind die Sicherungsdatenträger mit fortlaufenden Nummern versehen.

Datensicherung/Datensicherheit
Eine Datenmanipulation durch Malware wird mittels eingesetzter Antivirensoftware verhindert.

Von den Daten werden vor dem Transport Sicherungskopien angelegt. Daneben erfolgt eine Verschlüsselung der Daten vor dem Transport nach Stand der Technik.

Entsorgung und Vernichtung von Datenträgern
Bei zu vernichtenden Daten(trägern) erfolgt der Transport zum Entsorgungsunternehmen in verschlossenen Behältern. Das Entsorgungsunternehmen wurde sorgfältig ausgewählt und schriftlich auf Art. 28 DSGVO verpflichtet. Datenträger werden datenschutzgerecht entsorgt.

Telefax
Es gibt schriftlich fixierte Telefax-Regeln. Die Mitarbeitenden werden durch eine Dienstanweisung auf den korrekten Umgang mit Telefaxgeräten hingewiesen.

E-Mail
Es werden keine E-Mail-Server eingesetzt, die unverschlüsselt über das Internet erreichbar sind, da anderenfalls die Passwörter für SMTP und/oder mindestens TSL 1.2 abgehört werden könnten. Sensible Daten bzw. Dokumente mit personenbezogenen Daten werden über TeamBeam (Skalio GmbH) verschlüsselt versendet. Das Passwort wird über einen anderen Übertragungsweg (z.B. per SMS) übermittelt.

Mobile Endgeräte und mobile Datenträger
Es kommen dienstliche Notebooks zum betrieblichen Einsatz. Die Notebooks als solche sowie das jeweilige Betriebssystem sind mittels „BitLocker“ voll verschlüsselt.

Es kommen dienstliche Smartphones zum betrieblichen Einsatz. Die Smartphones und Handys können im Verlustfall per Fernwartung gelöscht werden.

Es kommen dienstliche USB-Sticks zum betrieblichen Einsatz. Die USB-Sticks sind containerbasiert mittels „BitLocker To Go“ verschlüsselt.

W-LAN
Es gibt betriebsinterne W-LAN-Zugänge. W-LAN-Zugänge und der gesamte drahtlose Datenverkehr werden nach Stand der Technik geschützt (WPA2, Anmeldung per RADIUS-Server). Die zusätzliche Anmeldung per RADIUS-Server sorgt dafür, dass nur befugte Personen Zugriff haben.

Das Standardpasswort für die Konfiguration des Access Points bzw. des Routers wurde geändert.

Für Gäste und externe Mitarbeitende steht zusätzlich ein physikalisch getrenntes W-LAN zur Verfügung.

Fernwartung
Es werden Fernwartungen durch den externen IT-Dienstleister durchgeführt und die Kenntnisnahme von personenbezogenen Daten ist nicht ausgeschlossen. Die Fernwartung umfasst sowohl die installierten Softwareanwendungen sowie auch die Benutzeradministration nebst Helpdesk. Die Zugangskontrolle erfolgt hierbei durch Benutzerkennung und Passwort. Der Übertragungsweg ist hierbei mittels SSL-Verschlüsselung abgesichert. Die Fernwartung wird protokolliert. Fernwartungen erfolgen ausschließlich über Computer, die über den gleichen Sicherheitsstandard verfügen wie die lokalen betrieblichen Computer.

Telearbeit und Heimarbeit („Homeoffice“)

Es findet Heimarbeit statt, es sei denn, diese wird durch den Auftraggeber vertraglich ausgeschlossen.

Eingabekontrolle
(Es sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.)

Protokollierung
Es findet eine Protokollierung sämtlicher Aktivitäten der Eingabe, Änderung und Löschung personenbezogener Daten auf Betriebssystemebene statt. Es werden alle Aktivitäten der Eingabe, Änderung und Löschung sämtlicher Benutzer protokolliert, auch die, der an sich nicht berechtigten. Hierzu zählen auch die Aktivitäten der Netzverwaltung und Heimarbeiter. Die Protokolldaten unterliegen einer strengen Zweckbestimmung.

Die Protokolldateien werden anlassbezogen im 4-Augen-Prinzip ausgewertet. Die Protokolle werden sicher aufbewahrt und in regelmäßigen, kurz bemessenen

Abständen mittels Überschreibens wieder gelöscht.

Richtlinien
Ein Berechtigungskonzept regelt die Eingabe, Veränderung und Löschung von Daten.

Die für die Erstellung von Datenträgern und der Bearbeitung von Daten Befugten werden in Dienstanweisungen festgelegt.

Berechtigungen
Für Eingabe, Löschung und Veränderung von Daten werden entsprechend Berechtigungen erteilt und dokumentiert.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
Auftragskontrolle
(Es sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)

Überprüfung des Auftragnehmers
Auftragnehmer werden unter besonderer Berücksichtigung von Art. 28 DSGVO (Auftragsverarbeiter) und somit der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. Aufträge werden grundsätzlich schriftlich erteilt.

Es finden von Beginn und dann regelmäßig Überprüfungen des Auftragnehmers statt, insbesondere ob dieser die vertraglichen Regelungen einhalten kann bzw. einhält und ob er darüber hinaus in jedem Fall nachweisen kann, dass ausreichende und geeignete Datensicherungsmaßnahmen getroffen wurden. Diese Prüfungen werden vor Ort durchgeführt oder mittels vom Auftragnehmer zur Verfügung gestellter Unterlagen (z.B. Zertifikate oder Urkunden). Diese Überprüfungen werden schriftlich dokumentiert. Der Datenschutzbeauftragte der GPTW Deutschland GmbH ist bei allen Verträgen sowie der Prüfung der ordnungsgemäßen Durchführung der Auftragsverarbeitung einbezogen.

Der Auftraggeber hat in diesem Zusammenhang Kenntnis von der Erklärung zur Verpflichtung auf Vertraulichkeit und Verschwiegenheit im Rahmen der Verarbeitung von personenbezogenen Daten (entsprechend Art. 28 Abs. 3 lit. b DSGVO und ggf. § 3 TTDSG, § 35 SGB I).

Die GPTW Deutschland GmbH ist auch selbst als Auftragnehmerin tätig.

Einbindung des Datenschutzbeauftragten
Der Datenschutzbeauftragte ist seit Bestellung bei allen Verträgen sowie bei der

Prüfung der ordnungsgemäßen Durchführung der Auftragsverarbeitung einbezogen und verfügt über eine Übersicht sämtlicher Fälle. Aus dieser Dokumentation sind die personellen Zuständigkeiten bei der verantwortlichen Stelle ersichtlich.

Vertragsinhalte
Es wird bei jedem Auftrag geprüft, welche rechtlichen Maßnahmen die Auftragsvergabe abstützen. Jede Auftragsverarbeitungsvereinbarung wird stets schriftlich abgeschlossen. Hierbei sind die zu erfüllenden technischen und organisatorischen Maßnahmen des Auftragnehmers Bestandteil der Vereinbarung. Auch sind die Kompetenzen und Pflichten zwischen Auftraggeberin und Auftragnehmer klar abgegrenzt, insbesondere ist in diesem Zusammenhang sichergestellt, dass sich der Auftraggeber eindeutig identifizieren muss und ihre Beauftragten befugt sind, dem Auftragnehmer Weisungen zu erteilen. Weisungen erfolgen stets schriftlich beziehungsweise bedürfen der Schriftform.

Es existieren detaillierte Regelungen der Auftragsverhältnisse und Formalisierungen des gesamten Auftragsablaufs, auch zum Einsatz von Unterauftragnehmer sowie eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten (speziell auch bei der Datensicherung und beim Transport von Datenträgern) bezüglich der Datenerhebung, Datenerfassung, Daten-verarbeitung, Prüfung und Wartung. Es ist ebenfalls schriftlich geregelt, wie mit Anfragen von Betroffenen umgegangen wird. Es wird in der Vereinbarung ebenfalls vorgeschrieben, wie der Auftragnehmer nicht mehr benötigte Unterlagen zu behandeln hat.

Nachweise
Eine Datenübergabe erfolgt stets gegen Nachweis/Quittung.

Verfügbarkeit und Belastbarkeit Art. 32 Abs. 1 lit. b EU-DSGVO), sowie Verfügbarkeitskontrolle und rasche Widerherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)
Verfügbarkeitskontrolle
(Es sind Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

Notfallkonzept
Sofern ein Störfall auftritt, meldet die/der den Störfall feststellende Mitarbeitende diesen unverzüglich dem externen IT-Dienstleister.

Es wird regelmäßig eine Risiko- und Schwachstellenanalyse durch den externen IT-Dienstleister durchgeführt, dabei festgestellte Schwachstellen werden unverzüglich beseitigt.

Für den Fall, dass wichtige Bestandteile des Netzwerks ausfallen, werden Hardwarekomponenten als Ersatz vorgehalten („cold standby“). Zudem kann mit der Aufnahme eines Notbetriebs zum Beispiel bei einem Serverausfall innerhalb eines vertretbaren

Zeitraums begonnen werden.

Datensicherung
Die Verantwortlichkeiten für die zentrale Datensicherung sind geregelt.

Die Sicherung erfolgt automatisch und wird somit faktisch erzwungen. Hierbei werden mehrfach täglich Snapshots, täglich ein inkrementelles Backup des Daten- und Systemstatus sowie wöchentlich ein Vollbackup des Daten- und Systemstatus erstellt. Die einwandfreie Lesbarkeit der angefertigten Sicherungen wird regelmäßig überprüft.

Die Backups werden zugriffssicher und verschlüsselt in sicherer Entfernung bei der techperts GmbH aufbewahrt („räumliche und logische Trennung"). Die mobilen Sicherungsdatenträger des manuellen Backups werden zudem in eine andere Brandschutzzone außerhalb der Geschäftsräume des Dienstleisters (Bankschließfach) ausgelagert.

Die Daten können auch beim Ausfall von Backup-Lesegeräten schnell wiederhergestellt werden. Zusätzlich werden die Server-Festplatten in einem RAID-System gespiegelt.

Die zentrale und einheitliche Beschaffung von Hard- und Software ist geregelt.

Virenschutz
Es werden Virenschutzprogramme eingesetzt. Diese erkennen auch unbekannte Schadsoftware mittels heuristischer Verfahren.

Eine Überprüfung verschlüsselter Dateien findet erst bei einer Entschlüsselung statt (also erst bei Zugriff auf die entsprechende Datei). In dem Moment greifen die Virenschutzprogramme (on access) ein. Um dies sicherzustellen, sind auf allen Clients und Servern Virenschutzprogramme installiert.

Updates der Virenschutzprogramme erfolgen automatisiert sofort bei Erscheinen beziehungsweise mehrmals täglich. Als zusätzliche Schutz-maßnahme werden SPAM-Filter für den E-Mail-Verkehr genutzt.

Brandschutz der PC-Arbeitsräume
In den Büroräumen herrscht ein striktes Rauchverbot. Zusätzlich befinden sich Brandmelder und Feuerlöscher in den PC-Arbeitsräumen. Die Feuerlöscher werden regelmäßig durch den Anbieter gewartet.

Schutz der Server
Der Zugangsbereich zu den Servern ist durch eine Brandschutztüre gesichert. Die Server sind mittels Brandmelder gesichert. Ein Feuerlöscher ist gut erreichbar im Serverraum installiert. Daneben befinden sich im DV-Bereich keine brennbaren Gegenstände wie Reinigungsmittel, Papier oder Vorhänge.

Die Serverkomponenten und Leitungen sind vor eintretendem Wasser geschützt, da sie sich mindestens 20 cm über dem Fußboden befinden.

Eine unterbrechungsfreie Stromversorgung (USV) sichert den Server sowie die zentralen Netzwerkkomponenten gegen einen unerwarteten Stromausfall ab und schützt zusätzlich vor Überspannungen. Die USV wird regelmäßig gewartet und getestet.

Im Serverraum herrscht ein generelles Ess- und Trinkverbot.

Die technischen und organisatorischen Maßnahmen (Art. 32 DSGVO) wurden in Zusammenarbeit mit dem externen Datenschutzbeauftragten – Herrn Daniel Schwaiger, isdacom GmbH, datenschutz@greatplacetowork.de, +49 2203 18 36 791 – in einem internen Audit aufgenommen und es wurde geprüft und sichergestellt, dass diese eingehalten werden. Darüber hinaus werden die Maßnahmen in regelmäßigen Abständen auf ihre Wirksamkeit hin geprüft.

Auf die konkrete Benennung von einzelnen Komponenten wurde aus Sicherheitsgründen bewusst verzichtet. Nichtsdestotrotz wurden diese erfasst und sind in der IT-Sicherheitsdokumentation aufgeführt.

11. Ansprechpartner

Bei Fragen bzw. für weitere Auskünfte zu Datenschutz und Datensicherheit wenden Sie sich bitte an:

Herr Dr. Christoph Justen
Datenschutzkoordinator
+49 221 933 35 151
cjusten@greatplacetowork.de

Herr Daniel Schwaiger
Datenschutzbeauftragter der GPTW Deutschland GmbH (extern)
isdacom GmbH
+49 2203 18 36 791
datenschutz@greatplacetowork.de