ANLAGE

Technische und organisatorische Maßnahmen
gemäß Art. 32 DSGVO

Organisation:

Hostway Deutschland GmbH
Am Mittelfelde 29
D-30519 Hannover
Germany
- nachfolgend HWD genannt -

vertreten durch die Geschäftsführer:
Dr. Achilleas Anastasiadis, Cord Bansemer und Ilja Kassühlke

Stand: 02.05.2018

Präambel

HWD kann im Rahmen der Leistungserbringung von HWD mit personenbezogenen Daten in Kontakt kommen. Dabei steht die Verarbeitung von personenbezogenen Daten nicht im Fokus der eigentlichen Leistungserbringung der HWD. Durch die erbrachten Dienstleistungen kann jedoch der technische Zugriff auf personenbezogene Daten des Kunden durch HWD nicht ausgeschlossen werden. Gemäß Artikel 32 DSGVO hat HWD technische und organisatorische Maßnahmen zu treffen wann immer personenbezogene Daten verarbeitet werden. Diese sind erforderlich um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten.

HWD erfüllt diesen Anspruch durch die im Folgenden dokumentierten Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

a. Zutrittskontrolle

Der Zugang zum Haupteingang der HWD sowie sämtlicher Nebeneingänge ist durch einen Zaun physikalisch beschränkt. Die Türen und Tore durch den Zaun sind immer verschlossen und können nur mit Transpondern von Mitarbeitern der HWD Vorort geöffnet werden. Darüber hinaus können das Haupttor

sowie der Haupteingang des Zauns via Klingel und daran gekoppelte manuelle Öffnungsfunktion durch HWD-Mitarbeiter im Network-Operation-Center (NOC) geöffnet werden.

Sämtliche Zugangswege zu Gebäudeeingängen der HWD sind via Videoüberwachung gesichert. Die Mitarbeiter des NOCs haben 24/7 eine Live-Darstellung aller Kameras auf dafür dedizierten Bildschirmen im NOC.

Die Zugänge zum Gebäude sind stets verschlossen und können von außen nur mit Sicherheitsschlüsseln geöffnet werden. Der Zugang zum Gebäude wird rund um die Uhr durch qualifizierte Mitarbeiter am zentralen Empfang / NOC überwacht und jeder Mitarbeiter, Kunde oder Lieferant muss sich am Empfang anmelden. Bei Anmeldung erhält der Besucher einen Besucherausweis den er bei Verlassen des Gebäudes wieder abzugeben hat. Besucher werden hierbei bereits über die Hausordnung unterrichtet. Besucher müssen entweder angemeldet sein oder über die Berechtigungen zu einer Eigenanmeldung verfügen. Die Authentizität von Besuchern wird mittels gültigem Lichtbildausweis überprüft. Besucher werden von einer Mitarbeiterin oder einem Mitarbeiter persönlich am Empfang abgeholt. Organisatorisch ist geregelt, dass Fremde sich im Gebäude niemals allein aufhalten oder frei bewegen dürfen.

Der Zutritt zu den Rechenzentrumsflächen ist über eine Zutrittskontrollanlage gesichert und nur Mitarbeitern der HWD alleine möglich. Für das Rechenzentrum Am Mittelfelde 29 ist diese Zutrittskontrolle als 2-Faktor-Authentifizierung ausgelegt. Jeder Zutritt wird protokolliert. Zutrittsprotokolle und Videoaufzeichnungen werden einmal täglich für die zurückliegenden 24 Stunden durch Mitarbeiter der HWD kontrolliert.

Außerhalb der Arbeitszeiten erfolgt die Überwachung der Räumlichkeiten durch eine Alarmanlage gemäß VDE-Norm. Meldungen der Anlage werden durch einen Sicherheitsdienst überwacht und nach einem dokumentierten Interventionsplan verfolgt. Bei sämtlichen technischen Räumlichkeiten, den Zugangswegen sowie für den Perimeterschutz besteht eine zusätzliche Videoüberwachung. Diese ist insbesondere in allen Räumlichkeiten des Rechenzentrums vorhanden und wird durch zusätzliche Bewegungssensoren unterstützt.

b. Zugangskontrolle

Unbefugten wird der Zugang zu Datenverarbeitungssystemen nicht gewährt. Der Zugang über Außenschnittstellen zu unseren EDV-Systemen ist durch eine Firewall geschützt. Sensible Dienste die nicht öffentlich erreichbar sein müssen werden durch den Einsatz eines VPN abgesichert. Öffentlich erreichbare Systeme, wie E-Mail oder Internetzugang werden über entsprechende Trennungen von anderen Diensten isoliert. HWD betreibt je nach Sicherheitsklassifikation diverse, teilweise physisch vollständig entkoppelte Netzwerke. Sämtliche Systeme sind passwortgeschützt und verfügen über benutzerspe-

zifische Zugänge. Gruppenzugänge werden nicht genutzt. Neben dem Einsatz starker Passwörter auf Basis interner Passwortvorgaben wird ein 2-Faktor-System zur Authentifizierung an sensiblen Systemen der HWD genutzt. Die Passwort-Richtlinien der HWD definiert neben der geforderten Passwortkomplexität auch Rahmenparameter wie das zwangsweise Neusetzen eines Passwortes in definierten Fristen sowie den Verbot der Wiederverwendung eines Passwortes. Die Detaillierung der Zugriffsberechtigungen zu dem Equipment des Vertragspartners erfolgt gemäß der Weisung des Auftraggebers auf Basis der von HWD zu erbringenden Leistungen. Gemäß der internen Richtlinien der HWD erfolgen je nach Systemart und Einstufung unterschiedliche Reaktionen auf Fehlversuche bei der Anmeldung. Neben der zeitweisen Sperrung, dem dynamischen Hinzufügen von Netzwerk-Sperren, oder der vollständigen Sperrung eines Zugangs erfolgt auch eine Protokollierung und Alarmierung.

c. Zugriffskontrolle

Der Zugriff auf Netzwerkverzeichnisse oder Systeme, in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Dabei muss jeder Benutzer sich mit personenspezifischen Zugangsdaten authentifizieren. Die initiale Zugriffsmöglichkeit ist, wo immer dies aufgrund der Funktion des Systems und den Vorgaben des Kunden realisiert werden kann, immer auf das interne Netzwerk der HWD beschränkt. Im Falle einer externen Einwahl (VPN) in die internen Netzwerke der HWD erhält der Mitarbeiter lediglich Zugriff auf für ihn relevante Netzbereiche. Im Falle eines externen Zugriffs erfolgt die Authentifizierung darüber hinaus auf Basis einer 2-Faktor-Authentifzierung. Für den Zugriff auf die Systeme und das Equipment des Kunden werden kundenindividuelle Maßnahmen mit dem jeweiligen Kunden abgestimmt. Die Allgemeinen Zugriffswege für den Zugriff eines HWD-Mitarbeiters auf Systeme oder Instanzen des Kunden – soweit der Beauftragung entsprechend – werden mindestens mittels starker Verschlüsselung abgesichert.

Mitarbeiter der HWD erhalten dabei auf Basis definierter Berechtigungen je Anwendung / System nur die notwendigen Berechtigungen. Es wird klar zwischen Administratoren einer Anwendung / eines Systems und weiteren Benutzergruppen unterschieden. Die Berechtigungen werden halbjährlich im Rahmen des internen Revisionsprozesses sowohl auf Notwendigkeit als auch auf korrekte Konfiguration überprüft.

d. Trennungskontrolle

HWD verarbeitet eigene personenbezogene Daten immer nur innerhalb der für die konkrete Aufgabe notwendigen Systeme und Prozesse. Im Rahmen der eigenen Verarbeitung von personenbezogenen Daten trennt HWD Test-Umgebungen von Produktiv-Umgebungen. Je nach erbrachter Leistung isoliert HWD Kundendaten entweder physisch (separate Hardware-Systeme, bspw. „Hosting dedizierter

Server“) oder logisch. Eine logische Isolierung kann hier je nach erbrachter Leistung unterschiedlich realisiert werden („Virtuelle Server“, „Mandantenfähige Software“). Eine darüberhinausgehende Trennungskontrolle für die Speicherung und Verarbeitung von personenbezogenen Daten im Rahmen der Auftragsverarbeitung obliegt dem Auftraggeber.

2. Integrität gem. Art. 32 Abs 1 lit. b DSGVO

a. Weitergabekontrolle

Personenbezogene Daten oder anderweitig vertrauliche Daten werden bei der Übertragung mindestens mittels einer Transportverschlüsselung verschlüsselt. HWD verfügt über eine interne Richtlinie zum Einsatz von Kryptographie-Verfahren mit klaren Vorgaben welche Kryptographie-Verfahren in welchen Konstellationen mit welchen technischen Details zulässig sind. Dabei orientiert sich HWD an den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie dem National Institute of Standards and Technology (NIST).

Darüber hinaus empfiehlt HWD bei der Übertragung von personenbezogenen Daten im Kundenkontakt zusätzlich eine dateibasierte Verschlüsselung zu verwenden. So wird auch eine temporäre Ablage der Daten auf HWD oder Kundenseite abgesichert. Dies setzt jedoch die technische Fähigkeit des Kunden zur Annahme oder Übermittlung einer entsprechend verschlüsselten Datei voraus. Soweit HWD diese Möglichkeit mit dem Kunden feststellt, wird HWD eine solche mit dem Kunden abgestimmte Methode zur dateibasierten Verschlüsselung verwenden.

HWD verfügt über einen Standard-Prozess zur Verwahrung sowie der Löschung oder physischen Vernichtung von Datenträgern. Hierbei werden sowohl der Datenträger als auch der sichere Verwahrort sowie die anschließende Rückübermittlung, Löschung, oder Vernichtung protokolliert. Die Vernichtung erfolgt gemäß Sicherheitsstufe H-4 DIN 66399-2.

Der Versand personenbezogener Daten erfolgt ausschließlich im gesetzlich vorgesehenen Rahmen. Mobile Datenträger mit personenbezogenen Daten werden nur in gesicherten Räumen gehalten, bei Nichtverwendung im Tresor. Daten, die für eine Auftragsdurchführung nicht mehr benötigt werden, wie z.B. gesperrte Daten, werden in einem separierten zugriffsgeschützten Speicherbereich abgelegt. Datenträger oder Hardware werden nur durch entsprechend verpflichtete und zertifizierte Unternehmen repariert oder entsorgt. Gleiches gilt für die Entsorgung von Daten auf Papier.

b. Eingabekontrolle

Nur ausgewählte Mitarbeiter können in einem Kundenprojekt auf die Systeme und Daten des Kunden

zugreifen. Dabei werden nur Mitarbeiter ausgewählt, die auch für die Erbringung der vertraglich zugesicherten Leistung direkt notwendig sind. Die Legitimation der Mitarbeiter ergibt sich aus der Zuordnung zur Gruppe der für diesen Kunden zuständigen Mitarbeiter. Alle Mitarbeiter sind dabei auf die Vertraulichkeit und Einhaltung der gesetzlichen sowie internen Regelungen verpflichtet.

Arbeiten an den Kundensystemen werden protokolliert. Wo technisch möglich erfolgt eine automatische Protokollierung aller Veränderungen und Aktionen. Darüber hinaus erfolgt eine manuelle Protokollierung der Mitarbeiter. Dies wird regelmäßig Stichprobenhaft überprüft.

Die Standard-Arbeitsanweisung an Mitarbeiter ist keine personenbezogenen Daten der Kunden zu verändern oder zu manipulieren. Dies darf nur auf explizite Weisung des Kunden erfolgen. Davon ausgenommen sind Regelprozesse zur Verwaltung von Daten (Datensicherung, Löschung von Protokolldaten nach vertraglich festgelegter Aufbewahrungszeit etc.), die im Rahmen des Betriebes der Kundeninstanzen in Standard-Logdateien der eingesetzten Serversoftware anfallen und ebenfalls personenbezogene Daten enthalten können.

3. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs 1 lit. b DSGVO

a. Verfügbarkeitskontrolle

HWD verfügt über zwei physisch voneinander unabhängige und räumlich getrennte Rechenzentren. Die Sicherstellung der Verfügbarkeit kundenspezifischer Daten erfolgt im Rahmen der vertraglich definierten Anforderungen. HWD betreibt hierfür Datensicherungsspeicher in beiden Rechenzentren, um Datensicherungen über Kreuz zu ermöglichen. Datensicherungsintervalle sind dabei individuell vertraglich mit dem Kunden gestaltbar. Für IT-Systeme und Daten der HWD, die zum Betrieb des Rechenzentrums und somit zur Sicherstellung der Verfügbarkeit von Kundensystemen und –daten ebenfalls notwendig sind, erfolgt eine tägliche über Kreuz-Sicherung mit zusätzlicher Sicherung aller geänderten Daten nachdem Arbeiten an den HWD-Systemen durchgeführt wurden. Darüber hinaus werden die Storage-Systeme, auf denen Kundensysteme betrieben werden, standardmäßig mit fehlertoleranten RAID-Systeme vor Datenverlust geschützt. Hier kann es je nach vertraglicher Individualkonfiguration bei Kunden jedoch Abweichungen geben. Für vom Auftraggeber von Dritten gemietete EDV-Systeme oder vom Auftraggeber eingestellte EDV-Systeme ist der Auftraggeber verantwortlich. Um das Ausmaß möglicher Brandschäden zu minimieren, ist unser Unternehmen mit einer Brandmeldeanlage ausgestattet. Meldungen der Anlage werden durch einen Sicherheitsdienst überwacht und nach einem dokumentierten Interventionsplan verfolgt. Die Klimaanlagen sind N+1 vorhanden und werden durch ein Notstromaggregat versorgt.
Beide Rechenzentrumsstandorte verfügen über USV-Systeme, sowie eine Notstromersatzanlage.
HWD betreibt im Rahmen eines aktiven Information Security Management Systems nach ISO-27001 auf Basis IT-Grundschutz eine aktive Notfallvorsorge. Hierzu gehört neben der kontinuierlichen Weiterent-

wicklung des Notfallhandbuchs auch die regelmäßige Durchführung von Notfallübungen. Diese erfolgen mindestens zweimal im Jahr und werden als detaillierte Planspiele umgesetzt. Mindestens einmal im Jahr erfolgt darüber hinaus ein sogenannter „Black Building Test“ um einen vollständigen Stromausfall zu simulieren. Die Durchführung der Übungen sowie der darin gewonnenen Erkenntnisse werden protokolliert.
HWD überwacht die Verfügbarkeit jeglicher Systeme zum Betrieb der Rechenzentren. Darüber hinaus überwacht HWD im Standard auch die Verfügbarkeit von Kundensystemen. Der Umfang dieses Monitorings wird dabei im Rahmen der Vertragsgestaltung / Angebotsphase durch den Kunden festgelegt und kann auch in einer bestehenden Vertragsbeziehung jederzeit angepasst werden. Neben einer zeitnahen Alarmierung bei Ausfall oder Störung entsprechender Systeme oder Anwendungen kann HWD so auch die Verfügbarkeit eines Systems oder einer Anwendung nachweisen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a. Datenschutz-Management

HWD betreibt ein Datenschutz-Management-System. Hierfür stellt HWD einen Datenschutzbeauftragten der das Datenschutz-Management-System betreut und direkt an die Geschäftsleitung berichtet. Im Rahmen des Datenschutz-Management-Systems dokumentiert HWD jegliche Verfahren und Prozesse mit Verarbeitung von personenbezogenen Daten in Unternehmensinternen Verfahrensverzeichnissen. Ebenso betreibt HWD ein ISMS nach ISO-27001 auf Basis IT-Grundschutz und ist nach diesem Standard durch das Bundesamt für Sicherheit in der Informationstechnik zertifiziert worden. Das Zertifikat wird in jährlichen Intervallen überprüft und alle 3 Jahre neu beantragt und geprüft. Technische organisatorische Maßnahmen werden jährlich überprüft, unter anderem auch im Rahmen der Zertifikatsüberprüfung.

Im Rahmen des Datenschutz-Management-Systems nimmt HWD bei identifizierten Bedarf Datenschutz-Folgenabschätzungen vor.

Darüber hinaus hat HWD alle Mitarbeiter zur Einhaltung der Vertraulichkeit und der Datenschutzgesetze schriftlich verpflichtet und erneuert diese Verpflichtung jährlich. Ebenso ist ein regelmäßiger Sensibilisierungs- und Schulungsprozess aller Mitarbeiter etabliert.

b. Incident-Response-Management

HWD betreibt im Rahmen des etablierten ISMS einen dokumentierten Prozess zum Incident-Response-Management. Neben Eskalations- und Meldewegen beinhaltet dieser Prozess die Nachbetrachtung

und Analyse und anschließende Optimierung auf Basis gewonnener Erkenntnisse.

Zur Erkennung von Incidents setzt HWD sowohl gerätebasierte als auch netzwerkbasierte Lösungen ein (Intrusion-Detection, Virus- und Malware-Erkennung, Anti-Spam-Filter sowie Anomalie-Detektionen). Darüber hinaus überwacht HWD die Infrastruktur und Kundensysteme mit einer Monitoring-Lösung auf Störungen und Anomalien.
Alle Incidents werden im Rahmen des Incident-Response-Management-Systems in einem Ticketsystem dokumentiert. Sowohl der Datenschutzbeauftragte (wenn personenbezogene Daten betroffen sind) als auch der IT-Sicherheitsbeauftragte sind im Rahmen des Eskalationsprozesses einzubinden.

c. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

HWD verfolgt das Prinzip der Datenminimierung. So werden nur Daten die für den jeweiligen Prozess / Kontext notwendig sind verarbeitet und gespeichert. Die Angemessenheit wird regelmäßig durch den Datenschutzbeauftragten geprüft. Alle Berechtigungen werden nach einem „Need-to-have“-Prinzip vergeben und müssen begründet werden. Die Vergabe von Berechtigungen wird regelmäßig im internen Revisionsprozess überprüft und hinterfragt.

Speicher- und Löschfristen werden aktiv definiert. Deren Einhaltung wird durch den Datenschutzbeauftragten geprüft.

d. Auftragskontrolle (Outsourcing an Dritte)

HWD prüft (Unter-)Auftragnehmer im Rahmen des Auswahlprozesses sowie in der kontinuierlichen Zusammenarbeit auf angemessene Datenschutz- und IT-Sicherheitsprozesse. Hierzu nimmt HWD neben einer Sorgfaltsprüfung im Auswahlprozess eines (Unter-)Auftragnehmers auch Stichprobenprüfungen (Dokumentation und Vor-Ort) bei (Unter-)Auftragnehmern vor.

HWD verpflichtet jegliche (Unter-)Auftragnehmer vertraglich sowohl auf die geltenden Vertraulichkeitsverpflichtungen als auch auf die Einhaltung des Datenschutzes. Entsprechend wird für alle (Unter-)Auftragnehmer mit Bezug zu personenbezogenen Daten eine Auftragsvereinbarung geschlossen.

Hostway Deutschland GmbH

- Die Geschäftsführung -