Technische und organisatorische Maßnahmen

Das nachfolgende Dokument dient nur der erläuternden Darstellung gesetzlicher Anforderungen in Bezug auf den Datenschutz. Die Rechte und Pflichten der Parteien ergeben sich allein aus den vertraglichen Vereinbarungen und den gesetzlichen Bestimmungen zum Datenschutz. Insofern können aus diesem Dokument keine Ansprüche abgeleitet werden. Technische Änderungen und/oder Änderungen in der Organisation, die keinen Einfluss auf die Erfüllung der gesetzlichen Anforderungen der DS-GVO in der jeweils aktuellen Fassung haben, bedürfen keiner gesonderten Information gegenüber dem Vertragspartner.

§ 1 Vertraulichkeit

1.1 Zutrittskontrolle

Darunter sind Maßnahmen zu verstehen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Büroräume der UNITED GRID befinden sich in einem Bürohaus in München. Die Zugänge zum Bürohaus und auch zu den Büroräumen der UNITED GRID sind Tag und Nacht verschlossen. Zugang zu dem Bürohaus haben nur der Vermieter und die Mieter der Büroräume. Es kommt ein elektronisches Schließsystem zum Einsatz, das vom Vermieter verwaltet wird. Nicht befugten Personen ist der Zutritt zu den Räumlichkeiten der München nicht gestattet. Sämtliche Personen, die Zutritt zu den Büroräumen erhalten, werden elektronisch erfasst.

Die Anwesenheit von Personen in den Räumlichkeiten der UNITED GRID wird über das elektronische Schlüsselsystem protokolliert.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten erst nach Türöffnung durch den Empfang Zutritt zu dem Bürohaus und dann den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.

Jeder Besucher wird in einem Besucherbuch protokolliert und dann von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet. Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

1.2 Zugangskontrolle

Durch die Zugangskontrolle wird verhindert, dass die Datenverarbeitungssysteme von UNITED GRID von Unbefugten genutzt werden können. Hält sich die bei Zutritt kontrollierte Person bereits in einem Raum auf, in dem sich die Datenverarbeitungsanlage der UNITED GRID befinden, wird sichergestellt, dass die betreffende Person diese Datenverarbeitungsanlage benutzen darf. Es ist jederzeit nachvollziehbar, wer wann welches Datenverarbeitungssystem benutzt hat.

Für die Zugangskontrolle sind nachfolgende Maßnahmen von UNITED GRID getroffen worden:

1.3 Zugriffskontrolle

Darunter sind Maßnahmen zu verstehen, die 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.

UNITED GRID stellt sicher, dass die berechtigte Personen ausschließlich auf die Daten zugreifen können, für die sie eine Zugriffsberechtigung besitzen (need-to-know-Prinzip) und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Zugriff auf personenbezogene Daten wird kontrolliert, indem dieser in Logdateien des Systems manipulationssicher protokolliert wird. Wenn sich eine befugte Person in einem Raum mit einer Datenverarbeitungsanlage befindet und das System benutzt, ist sichergestellt sein, dass sie nur auf die Daten zugreifen kann, für die sie die entsprechende Berechtigung besitzt (Berechtigungskonzept). Dabei ist nachvollziehbar sein, wer wann auf welche Daten zugegriffen hat.

Berechtigungen für IT-Systeme und Applikationen der UNITED GRID werden ausschließlich von Administratoren eingerichtet. Voraussetzung für eine Berechtigung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Der Antrag kann auch bei der Personalabteilung gestellt werden.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten. Zusätzlich kann eine Freigabe für einzelne Dateien im Bedarfsfall durch den Administrator vorgenommen werden. Um eine Freigabe einzuräumen, muss ein Antrag durch den Vorgesetzten bzw. den Geschäftsführer vorliegen.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet. Alle Mitarbeiter bei UNITED GRID sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.

Für die Verarbeitung von personenbezogenen Daten sind die Beschäftigten von UNITED GRID verpflichtet nur auf getestete und freigegebene Anwendungssoftware zurückzugreifen. Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.

Personenbezogene Daten werden auf sicheren DS-GVO konformen Datenservern gespeichert. Das Speichern von Daten auf lokale Datenträger ist nicht vorgesehen. Eine lokale Speicherung von Daten auf einem lokalen Datenträger erfordert die Freigabe durch den Vorgesetzten.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

1.4 Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich nur über verschlüsselte Verbindungen.

Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Verschlüsselungssysteme im Einsatz.

§ 2 Integrität

2.1 Weitergabekontrolle

Maßnahmen, die 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.

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von UNITED GRID erfolgt, darf jeweils nur in dem Umfang, wie erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten grundsätzlich untersagt. Beim Ausscheiden der Mitarbeiter werden eventuell bestehende Zugriffsrechte zur Weitergabe von Daten aufgehoben.

Mitarbeiter bei UNITED GRID werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

§ 3 Verfügbarkeit und Belastbarkeit

Die UNITED GRID stellt sicher, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Die Verfügbarkeit der Daten wird regelmäßig kontrolliert, d. h. es wird sichergestellt, dass die personenbezogenen Daten zu festgelegten Zeiten im festgelegten Umfang zur Verfügung gestellt werden. Die Verfügbarkeit selbst entspricht dabei den rechtlichen und betrieblichen Erfordernissen, so dass u. a. bei Wartungsfenstern für die Pflege und Wartung der Systeme und Software, diese den laufenden Betrieb nicht negativ beeinflussen.

UNITED GRID nutzt für die Speicherung und Verwaltung von personenbezogen Daten sowie für die Bereitstellung von Servern einen Cloud-Dienstleister und betreibt in den eigenen Räumlichkeiten keine eigenen Servern. UNITED GRID stellt dabei viertjährlich die Eignung und Sicherheit der zu Verfügung gestellten Dienste sicher und prüft eventuell vorliegende Zertifizierung durch die eingesetzten Prüfstellen.

3.1 Sicheres Design

Sämtliche Daten der UNITED GRID werden verschlüsselt gespeichert, sowohl wenn sie sich auf einem lokalen Datenträger befinden, auf Sicherungsmedien gespeichert werden, oder wenn sie über das Internet übertragen werden.

Sämtliche Daten werden stets mehrfach redundant gespeichert, das heißt die Daten liegen gespiegelt vor.

Daten auf den Serversystemen von UNITED GRID werden mindestens monatlich inkrementell und monatlich vollständig gesichert. Die Sicherungsdaten werden verschlüsselt und in einem virtuell abgetrennten Cloud-Speicher separat gespeichert und verwaltet. Das Einspielen von Backups wird regelmäßig getestet.

Die eingesetzten Rechenzentren sind darauf ausgelegt, Funktionsausfälle zu antizipieren und zu tolerieren und dabei Servicelevel aufrecht zu erhalten. Für das Eintreten eines Funktionsausfalls wird der Datenverkehr von dem vom Ausfall betroffenen Bereich auf einen anderen umgeleitet. Kommt es in einem Rechenzentrum zu einem Funktionsausfall, stehen genügend Kapazitäten zur Verfügung, damit der Datenverkehr auf die verbleibenden Standorte aufgeteilt werden kann.

3.2 Überwachung und Erkennung

Physische Zugangspunkte zu Serverräumen werden von CCTV-Kameras mit Aufzeichnungsfunktion überwacht. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt.

Der physische Zugang wird durch professionelles Sicherheitspersonal an den Gebäudeeingängen kontrolliert. Dabei werden Überwachung, Meldeanlagen und andere elektronische Vorrichtungen eingesetzt. Autorisiertes Personal erlangt über Multi-Faktor-Authentifizierungsmechanismen Zugang zu den Rechenzentren. Die Eingänge zu den Serverräumen sind mit Geräten abgesichert, die Alarm auslösen, wenn die Tür aufgebrochen oder offen gehalten wird.

In der Datenebene sind elektronische Einbruchmeldesysteme installiert, die sicherheitsrelevante Ereignisse erkennen und automatisch die zuständigen Mitarbeiter alarmieren. Die Ein- und Ausgänge der Serverräume sind durch Geräte gesichert, an denen Personal Multi-Faktor-Authentifizierungsverfahren durchlaufen müssen, bevor sie den Raum betreten oder verlassen können. Diese Geräte lösen einen Alarm aus, wenn die Tür ohne Autorisierung aufgebrochen oder offen gehalten wird. Die Türalarmsysteme sind so konfiguriert, dass sie erkennen, wenn jemand eine Datenebene ohne Multi-Faktor-Autorisierung betritt oder verlässt. In diesem Fall wird umgehend ein Alarm ausgelöst.

3.3 Gerätemanagement

Medienspeichergeräte, auf denen personenbezogene gespeichert sind, werden vom Betreiber der Datencenter als kritisch eingestuft und deshalb über ihren gesamten Lebenszyklus als höchst dringlich behandelt. Der Betrieber hat bestehende Normen, wie die Geräte installiert, betrieben und irgendwann zerstört werden, wenn sie nicht mehr verwendet werden. Wenn ein Speichergerät das Ende seines Lebenszyklus erreicht hat, wird es gemäß zertifizierter Techniken stillgelegt. Medien, auf denen Kundendaten gespeichert wurden, werden erst nach erfolgter Stilllegung aus der Hand gegeben.

3.4 Betriebliche Support-Systeme

Die elektrischen Anlagen der eingesetzten Rechenzentren wurden so entwickelt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs gewartet werden können. Dabei ist sichergestellt, dass die Rechenzentren mit einer Notstromversorgung ausgestattet sind, damit im Fall eines Stromausfalls der Betrieb von kritischen Lasten der Anlage gewährleistet ist.

Die genutzten Rechenzentren verfügen über Klimaanlagen zur Kontrolle der Betriebstemperatur für Server und andere Hardware, um eine Überhitzung zu vermeiden und das Risiko von Serviceausfällen zu verringern. Temperatur und Luftfeuchtigkeit werden in angemessener Weise vom Personal und den technischen Systemen überwacht und geregelt.

Die Rechenzentren sind mit automatischen Geräten zur Branderkennung und -bekämpfung ausgestattet. Die Branderkennungssysteme setzen Rauchsensoren in vernetzten, mechanischen und Infrastrukturbereichen ein. Diese Bereiche sind darüber hinaus durch Brandbekämpfungssysteme geschützt.

Um Wasserlecks erkennen zu können, sind die Rechenzentren mit Wassererkennungssensoren ausgestattet. Wenn Wasser entdeckt wird, wird dieses entfernt, um zusätzliche Wasserschäden zu vermeiden.

3.5 Governance und Risiko

Die von UNITED GRID eingesetzten Rechenzentren sind darauf ausgelegt, Funktionsausfälle zu antizipieren und zu tolerieren und dabei Servicelevel aufrecht zu erhalten. Für das Eintreten eines Funktionsausfalls wird der Datenverkehr von dem vom Ausfall betroffenen Bereich auf einen anderen umgeleitet. Für wichtige Anwendungen gilt ein N+1-Standard. Kommt es in einem Rechenzentrum zu einem Funktionsausfall, stehen genügend

Kapazitäten zur Verfügung, damit der Datenverkehr auf die verbleibenden Standorte aufgeteilt werden kann.

Kritische Systemkomponenten werden an mehreren, voneinander isolierten Standorten (Availability Zones genannt) gesichert. Jede Availability Zone ist auf einen unabhängigen Betrieb mit hoher Zuverlässigkeit ausgelegt. Die Availability Zones sind vernetzt. Dies ermöglicht Ihnen die Nutzung von Anwendungen, für die ein automatischer, unterbrechungsfreier Failover zwischen den Availability Zones eingerichtet ist. Extrem ausfallsichere Systeme und eine daraus resultierende Serviceverfügbarkeit sind Bestandteil des Systemdesigns.

Es werden zudem regelmäßig Bedrohungs- und Schwachstellenprüfungen der Rechenzentren durch den Betreiber durchgeführt. Die fortlaufende Bewertung und Abwehr von potenziellen Schwachstellen erfolgt über die Risikobewertungsaktivitäten der Rechenzentren. Dabei werden auch regionale behördliche und Umweltrisiken berücksichtigt.

Ein Betriebskontinuitätsplan des Betreibers umfasst Maßnahmen zur Vermeidung und Verringerung von Störungen durch Umwelteinflüsse. Der Plan enthält betriebliche Details zu den Maßnahmen, die vor, während und nach einem entsprechenden Ereignis ergriffen werden. Der Betriebskontinuitätsplan wird durch Tests gestützt, die auch Simulationen verschiedener Szenarios umfassen.

§ 4 Auftragskontrolle

Im Rahmen der Auftragskontrolle wird gewährleistet, dass personenbezogenen Daten, die im Auftrag verarbeitet werden, nur auf Grundlage des Vertrages entsprechend den Weisungen des Auftraggebers (Verantwortlichen) verarbeitet werden.

Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union.

Bei der UNITED GRID ist ein betrieblicher Datenschutzbeauftragter benannt.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführten Audit durch den Datenschutzbeauftragten von UNITED GRID abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

§ 5 Datenschutzfreundliche Voreinstellungen

Bei UNITED GRID wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirmmasken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder teilweise deaktiviert werden.

Die Software von UNITED GRID unterstützt sowohl die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von

Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen für Daten oder Funktionaliäten können flexibel und granular gesetzt werden.

§ 6 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

Bei UNITED GRID ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.

Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.