Vereinbarung gemäß Artikel 28 Absatz 3 DSGVO zur Auftragsverarbeitung personenbezogener Aktionärsdaten

Zwischen

Firma <Gesellschaft>
<Strasse> in <PLZ> <Ort>
vertreten durch <Vorstand>
im Folgenden Auftraggeber genannt

und

Firma namensaktie.de GmbH
Robert-Matzke-Str. 9 in 01127 Dresden
vertreten durch den Geschäftsführer Andreas Börnig
im Folgenden Auftragnehmer genannt

wird ergänzend zum bestehenden Dienstleistungsvertrag vom
<Vertragsbeginn>
Folgendes vereinbart:

§1
Einleitung, Geltungsbereich, Definitionen

1. Diese Vereinbarung regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden "Parteien" genannt) im Rahmen einer Verarbeitung von personenbezogenen Aktionärsdaten im Auftrag.
2. Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
3. In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden "schriftlich" zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

§2
Gegenstand und Dauer des Auftrags

1. Der Auftragnehmer übernimmt folgende Aufgaben:
   - Bereitstellung einer Datenbank zur Speicherung personenbezogener Daten nebst webbasiertem User-Interface mit rollenabhängigen Zugriffsmöglichkeiten.
   - Speichern und Verarbeiten personenbezogener Aktionärsdaten zur Erfüllung der Registrierungsvorschriften nach §67 AktG und weiterer gesetzlicher Anforderungen bei der

Gesellschafterverwaltung (Steuer, Statistik, Dokumentation der Hauptversammlung, Stimmabgaben, etc.).

- Speichern und Verarbeiten personenbezogener Daten zur Vorbereitung auf eine Aktionärseigenschaft.
- Speichern und Verarbeiten personenbezogener Daten zur Sicherstellung eines kontrollierten und protokollierten Zugriffs auf die Aktionärsdaten durch autorisierte Personen.
- Protokollierte Eingabe, Aktualisierung oder Löschung personenbezogener Daten auf Weisung des Auftraggebers.

2. Die Auftragsverarbeitung beginnt mit Inkrafttreten des Dienstleistungsvertrags (im Folgenden "Hauptvertrag" genannt) und erfolgt auf unbestimmte Zeit. Sie kann durch Kündigung des Hauptvertrages beendet werden. Der Auftragnehmer ist nach Kündigung verpflichtet, die Auftragsverarbeitung bis zur ordnungsgemäßen Abwicklung der Datenrückgabe weiterzuführen.

§3
Konkretisierung von Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

1. Die Verarbeitung ist folgender Art:
   - Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten

2. Es werden folgende Daten verarbeitet:
   - Personenstammdaten (z.B.: Name, Anschrift, Geburtsdatum)
   - Kommunikationsdaten (z.B.: Telefon, E-Mail, Fax, Homepage)
   - Zugangsdaten (z.B.: Passwörter [salted], Public-Keys, Log-Daten)
   - Aktionärs-typische Daten (z.B.: Bestand, Zugang, Abgang, Stimmrechte)
   - AG-Verwaltungs-typische Daten (z.B.: Weisungen, Stimmrechtsvertreter, Abstimmergebnisse)
   - Steuer erforderliche Daten (z.B.: KiStAM-Daten)
   - Handelsunterstützende Daten (z.B.: Angebote, Nachfragen)
   - AG-Stammdaten
   - Vorgenannte Daten als Historie (mit Vermerk: "gültig von" und "gültig bis")

3. Von der Verarbeitung sind folgende Personenkategorien betroffen:
   - Aktionäre
   - Potentielle Aktionäre
   - Registerführer und Controller des Auftraggebers
   - Administratoren des Auftragnehmers

§4
Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

3. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format (z.B.: E-Mail). Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format (z.B.: E-Mail) zu bestätigen. Die Formulierung der mündlichen Weisung kann auch durch den Auftragnehmer per E-Mail erfolgen. In diesem Fall reicht als Bestätigung ein short reply.

4. Der Auftraggeber ist berechtigt, sich wie unter § 6 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§5
Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

1. Weisungsberechtigte Personen des Auftraggebers sind:

    - Der aktuell im Bundesanzeiger bekannt gemachte Vorstand.
    - Im Falle einer Insolvenz, der legitimierte Insolvenzverwalter.
    - Personen, die von vorgenannten Weisungsberechtigten durch Zuteilung der Rolle "Registerführer-A" im Aktienregister autorisiert wurden.

2. Weisungsempfänger beim Auftragnehmer sind:

    - Der Geschäftsführer des Auftragnehmers.
    - Personen, die vom Geschäftsführer des Auftragnehmers durch Zuteilung der Rolle "Admin" im Aktienregister autorisiert wurden.

§6
Technisch-organisatorische Maßnahmen

1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (siehe Anhang 1 "Technisch-organisatorische Maßnahmen"). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die

Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

2. Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Eine Dokumentation der technischen und organisatorischen Maßnahmen ist als Anlage 1 Bestandteil dieser Vereinbarung.

§7
Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§8
Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.
   Als Ansprechpartner beim Auftragnehmer wird Herr Andreas Börnig, Robert-Matzke-Str. 9, 01127 Dresden, Tel.: 0351-40765085, E-Mail: boernig@namensaktie.de, benannt.

2. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO.
   Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 1).

4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der

Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

6. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

7. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

8. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Paragraf 10 dieses Vertrages.

§9
Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

2. Die Parteien sind sich darüber einig, dass der Auftragnehmer die zum Betrieb des Aktienregisterservers erforderliche Hardware in einem zu der Hetzner Online GmbH (Industriestr. 25, D-91710 Gunzenhausen, https://www.hetzner.de) gehörigen Rechenzentrum anmieten darf.
   In diesem Fall versichert der Auftragnehmer, dass er die alleinige Kontrolle über Betriebssysteme, Software und Datenbanken besitzt und ein Zugriff auf Daten des Auftraggebers durch Mitarbeiter der Firma Hetzner, auch im Falle eines Tauschs defekter Hardwarekomponenten (z.B.: Festplatten), durch geeignete Virtualisierungs- und Verschlüsselungstechnologien, die nach dem allgemeinen Kenntnisstand als sicher gelten, unterbunden wird (technische Einzelheiten in Anlage 1).
   Der Auftragnehmer versichert, dass er sich von der Zertifizierung nach ISO 27001 (siehe Anlage 2) und Zuverlässigkeit der Firma Hetzner überzeugt hat und bei dieser seit 2008 ohne Probleme oder nennenswerte Systemausfälle Hostrechner für den Betrieb von Aktienregisterservern anmietet.

3. Weitere Unterauftragnehmer (weitere Auftragsverarbeiter) darf der Auftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

§10
Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO im Rahmen des Möglichen überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und die Umsetzung der technischen und organisatorischen Maßnahmen, soweit möglich, nachzuweisen.

3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO erfolgen..

4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§11
Mitteilung bei Verstößen des Auftragnehmers

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
   a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
   b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
   c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
   d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
   e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§12
Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber in einem allgemein üblichen Datenbank-Export-Format (z.B.: CSV) auszuhändigen. Nach vorheriger Zustimmung durch den Auftraggeber sind anschließend die Datenbestände datenschutzgerecht zu löschen bzw. zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage 1: Technisch-organisatorische Maßnahmen

Serverarchitektur und physischer Serverstandort

Jede Aktiengesellschaft verfügt über einen eigenen virtuellen Aktienregisterserver mit individuell konfigurierbarer Programmlogik und exklusivem Zugangsport für den Datenaustausch. Der Aktienregisterserver speichert die Aktionärsdaten über einen marktüblichen Open-Source-Datenbankserver in einem zugangsbeschränktem Datenbankbereich. Die Ports der Aktienregister- und Datenbankserver sind nicht über das Internet erreichbar.

Die Anbindung der Aktienregisterserver an das Internet erfolgt über einen als Proxy und der Verschlüsselung dienenden Open-Source Apache-Webserver, der auf dem aktuellen Sicherheitsstand gehalten wird. Dieser ermöglicht einen Zugang über den Standard-http-Port 80 und den Standard-https-Port 443. Die Öffnung des Ports 80 dient dem alleinigen Zweck, einen sofortigen redirect auf den verschlüsselten Port 443 auszulösen, so dass stets eine gesicherte Verbindung für den Informationsaustausch zwischen Anwender und Aktienregisterserver sichergestellt wird. Der Apache-Port 443 leitet Anfragen, die aufgrund ihrer Kennung einer Aktiengesellschaft zugeordnet werden können, an den entsprechenden lokalen Port des Aktienregisterservers - oder bei Lastverteilung an den Apache-Webserver eines gleichartigen Systems - weiter. Alle anderen Anfragen werden zurückgewiesen oder auf eine Impressumseite umgeleitet.

Die Administration des Systems und die Weiterleitung verschlüsselter Backup-Dateien erfolgt über eine gesicherte SSH-Verbindung. Zu diesem Zweck ist ein vom Standardport 22 abweichender (und hier nicht näher genannter) Port geöffnet, auf dem ein Open-Source-SSH-Server, der auf dem aktuellen Sicherheitsstand gehalten wird, lauscht. Der Zugang über den SSH-Server ist ausschließlich durch das Public-Key-Verfahren möglich, alle anderen Anfragen werden zurückgewiesen.

Die vorgenannte Architektur befindet sich auf virtualisierten, vollverschlüsselten, minimalistischen Linux-Serverinstallationen (virtuelle Maschinen), die auf dem aktuellen Sicherheitsstand gehalten werden. Sämtliche Ports, mit Ausnahme von 80, 443 und dem nicht näher genannten SSH-Port, sind für das Internet geschlossen.

Der Betrieb der virtuellen Maschinen erfolgt auf Hostrechnern, die an einem Standort in Deutschland oder Finnland bei dem Rechenzentrumsbetreiber "Firma Hetzner Online GmbH" (siehe §9 Absatz 2.) angemietet werden. Die erforderlichen Betriebssysteme werden ausschließlich vom Auftragnehmer installiert und gewartet. Es kommen ebenfalls minimalistische Linux-Serverinstallationen zum Einsatz, die auf dem aktuellen Sicherheitsstand gehalten werden. Die Hostrechner dienen ausschließlich dem Betrieb virtueller Maschinen des Auftragnehmers und sind nur für autorisierte Personen des Auftragnehmers über den Admin-SSH-Port (wie auf vorbeschriebenen Systemen) zugänglich. Alle anderen Ports sind auf den Hostrechnern für das Internet geschlossen. Der Betrieb virtueller Maschinen mit administrativem Zugang durch Fremdpersonen (nicht zum Auftragnehmer gehörend) ist ausgeschlossen, so dass die Gefahr eines Datenabflusses durch denkbare Sicherheitslücken (z.B.: Meltdown, Spectre) aufgrund unzureichend abgeschotteter Arbeitsspeicherbereiche minimiert wird.

Zugangskontrolle und Protokollierung

Aktionärsdaten werden ausschließlich in einer AG-spezifischen Datenbank, die sich auf dem virtualisierten Serversystem befindet, gespeichert. Eingaben, Änderungen oder Löschungen sind nur über den Internetzugang des Aktienregisterservers nach einer protokollierten Zugangskontrolle möglich. Bei dem Kennung/Passwort-basierten LogIn-Verfahren werden eine E-Mail-Adresse oder Urkundenkennnummer gegen ein salted-hashed-Passwort geprüft und bei positivem Ergebnis ein rollenabhängiger Berechtigungsvermerk in die Session geschrieben. Mehrere Fehlversuche beim LogIn-Prozess führen zu

einer vorübergehenden Sperrung der anfragenden IP-Adresse. Eine Löschung der Session erfolgt automatisch nach längerer Inaktivität oder Wechsel der IP-Adresse.
Das mit https gesichert übertragene Klartextpasswort wird unmittelbar nach dem salted-hash-Vorgang aus dem Arbeitsspeicher gelöscht und in Interimslogfiles nur als Variable ohne Wert geschrieben. Interimslogfiles der Funktionsaufrufe und Formulareingaben werden für einen begrenzten Zeitraum auf dem Aktienregisterserversystem und einem räumlich getrennten Logfilesicherungsserver gespeichert und im Bedarfsfall für eine Analyse oder gegebenenfalls manuelle Korrektur von Störfällen genutzt.
Dauerhafte Protokolle (Nutzer, Datum, Rolle, IP-Nummer, Funktionsaufruf) werden bei den meisten Eingabe- und Änderungsvorgängen automatisch angelegt (Automatikbeleg), logisch verknüpft und in der Datenbank gespeichert.

Verschlüsselung und Backups

Aktienregisterserver, Datenbankserver und temporäre Backupspeicher werden ausschließlich auf virtuellen Maschinen betrieben (siehe Serverarchitektur), die im Ruhezustand vollverschlüsselt sind. Ein Zugriff auf entschlüsselte Speicherbereiche ist nur im kontrolliert laufenden Betrieb möglich.
Das Starten einer virtuellen Maschinen erfolgt in zwei Schritten. Der pre-boot-Modus dient der Bereitstellung eines SSH-Servers, der nach einer Public-Key-Autorisierung die manuelle Eingabe einer mindestens 32 Byte langen Passphrase zum Entschlüsseln des Hauptsystems ermöglicht. Nach Eingabe der korrekten Passphrase wird das Dateisystem entschlüsselt, der Bootvorgang fortgesetzt und der Interims-SSH-Server beendet. Die Autorisierung zur Eingabe der Passphrase ist auf zwei Personen beschränkt, die Passphrase selbst nur biologisch gespeichert.

AG-spezifische Datenbank-Backups werden einmal täglich erstellt und vor der Speicherung über einen Pipe-Operator synchron mit AES-256 verschlüsselt. Die Erstablage erfolgt auf dem Aktienregisterserversystem. Von dort werden die verschlüsselten Backup-Dateien in regelmäßigen Abständen über den SSH-Zugang an mindestens einen räumlich getrennten Archivspeicherort kopiert.
Zusätzlich werden in regelmäßigen Abständen komplette Systembackups der virtuellen Maschinen erstellt und vollverschlüsselt an einem räumlich getrennten Archivspeicherort abgelegt.

Datenverarbeitung in den Geschäftsräumen des Auftragnehmers

Registrierungstätigkeiten durch den Auftragnehmer erfolgen ebenfalls nur protokolliert über den Aktienregisterserver (siehe "Zugangskontrolle und Protokollierung"). Soweit eine manuelle Vorbereitung von Aktionärsdaten (z.B.: Umformatieren von Excel-Tabellen, Umkodieren von CSV-Dateien, Extrahieren von Daten aus Word-Dokumenten u.s.w.) durch den Auftragnehmer erforderlich ist, erfolgt dies auf Linux-Systemen, die auf dem aktuellen Stand gehalten werden.
Kundendaten werden ausschließlich in synchron mit AES-256 verschlüsselten Dateicontainern abgelegt, die nur nach manueller Eingabe einer Passphrase entschlüsselt werden können. Es wird konsequent darauf geachtet, dass auch bei kurzfristiger Abwesenheit des Sachbearbeiters der Dateicontainer verschlossen wird. Sicherheitskopien des verschlossenen Dateicontainers werden regelmäßig an räumlich getrennten Orten gespeichert. Ein Öffnen der Container außerhalb der Geschäftsräume ist nicht vorgesehen.

Sofern aus Kompatibilitätsgründen der Einsatz eines Windows-Systems unvermeidbar ist, erfolgt die Verarbeitung ausschließlich auf einer virtualisierten Rechnerumgebung ohne Internetanbindung. Diese wird von der Kopie eines fixen Snapshots auf einem Linux-Hostsystem gestartet. Nach Beendigung des Windows-Systems wird die Kopie des Snapshots komplett gelöscht.

Kommunikation und Datenaustausch zwischen Auftragnehmer und Auftraggeber

VERSCHLÜSSELUNG
Der Auftragnehmer unterstützt die gängigen asyncronen Verschlüsselungsverfahren mit PGP und Open-SSH. Die Bereitstellung bzw. Entgegennahme der entsprechenden public-Keys für die Verschlüsselung wird zugesichert.

HTTPS-UPLOAD
Auf jedem Aktienresgisterserver steht dem Vorstand ein Uploadformular zur Verfügung, das einen https-gesicherten Dateiupload auf den Server ermöglicht und von dort, über den Admin-SSH-Zugang, gesichert in die Geschäftsräume übertragen werden kann.

UNVERSCHLÜSSELT
Beim unverschlüsselten E-Mail-Austausch wird der Transportweg als nicht geschützt betrachtet. Gleichwohl erfolgt der Umgang mit den auf diese Art übergebenen Daten und Informationen, nach dem Eingang auf Rechnern in den Geschäftsräumen des Auftragnehmers, wie unter "Datenverarbeitung in den Geschäftsräumen" beschrieben.

Risikoanalyse von Störfällen

UNKONTROLLIERTER STROMAUSFALL
Eine unkontrollierte Stromunterbrechung führt zu einem schlagartigen Ausfall des Hostrechners und der virtuellen Maschinen. Die Systeme sind darauf konzipiert, einen Datenverlust wegen nicht abgeschlossener Schreibvorgänge auf den Festplatten mit großer Wahrscheinlichkeit auszuschließen. Zusätzlich erfolgt nach einem unkontrollierten Serverneustart automatisch ein Datenbankintegritätstest. Das Hostsystem ist gegen Probleme dieser Art gesondert abgesichert.

Nach Wiederherstellung der Stromversorgung wird der Hostrechner automatisch gestartet und versetzt anschließend - ebenfalls automatisch - die virtuellen Maschinen in den pree-boot-Modus, der eine manuelle Entschlüsselung der Dateisysteme, wie unter "Verschlüsselung und Backups" beschrieben, ermöglicht. Über die Notwendigkeit einer administrativen Entschlüsselung der virtuellen Maschinen wird durch die automatisierte E-Mail eines unabhängigen, regelmäßig testenden Kontrollservers oder eine Kundenanfrage informiert. Nach Entschlüsselung werden die virtuellen Maschinen, sowie die darauf laufenden Aktienregisterserver, automatisch gestartet und einem Datenbankintegritätstest unterzogen. Bei Problemerkennung wird der entsprechende Server gesperrt und ein Admin automatisch per E-Mail informiert. Überprüfung und gegebenenfalls Reparatur erfolgen in diesen Fällen manuell.

UNTERGANG ODER DIEBSTAHL
Ein Untergang durch Feuer, Terroranschlag oder Naturkatastrophe führt in der Regel zu einer Komplettvernichtung der Datenspeicher oder zu einem Ausfall des Hostrechners, was ein Auslesen der Datenspeicher ohne vorherige Entschlüsselung ebenfalls unmöglich macht.

Bei einem Diebstahl ohne Unterbrechung der Stromversorgung bleiben die Schutzmaßnahmen vor unberechtigten Zugriffen, wie unter "Zugangskontrolle und Protokollierung" beschrieben, unverändert erhalten.
Ein Diebstahl mit Stromunterbrechung (wahrscheinlichere Variante) hinterlässt vollverschlüsselte Datenspeicher, die ohne administrative Entschlüsselung (siehe: "Verschlüsselung und Backups") keinen Zugriff auf Kundendaten ermöglichen.

In den zuvor genannten Fällen ist davon auszugehen, dass die Serverarchitektur komplett neu aufgesetzt werden muss. Für die kurzfristige Anmietung geeigneter Hostrechner stehen in Deutschland neben der

Hetzner Online GmbH mehr als fünf unabhängige Rechenzentrumsbetreiber zur Verfügung. Die Vorbereitung eines Hostrechners (Installation von Betriebssystem, Virtualisierungssoftware, SSH-Zugang und Start-Scripten) ist eine geprobte Standardprozedur, die weitestgehend unabhängig von der verwendeten Hardware durchgeführt werden kann. Die erforderliche Installation der virtuellen Maschinen erfolgt durch einfaches Kopieren der Systembackups von dem externen Archivspeicherort mit anschließendem Restart des Hostrechners. Die Aktualisierung der AG-Datenbanken vom Zeitpunkt der Erstellung des Systembackups bis zum Zeitpunkt der letzten Datenbanksicherungen erfolgt durch manuelles Entschlüsseln und Einspielen der Datenbankbackups von dem externern Archivspeicherort. Eventuelle Mitteilungen an den Auftraggeber über erforderliche Neueingaben ab dem Zeitpunkt der letzten Datenbanksicherung bis zum Untergang des Systems werden nach einer Analyse des Logfilesicherungsservers (siehe: "Zugangskontrolle und Protokollierung") im Bedarfsfall ausgelöst. Zusätzlich wird der Auftraggeber über eine eventuell kurzfristig notwendige (bis zur vollständigen Verteilung der neuen IP-Nummer auf den DNS-Servern), manuelle Auflösung der Serverdomain informiert.

TAUSCH DEFEKTER HARDWAREKOMPONENTEN

Der Tausch defekter Hardwarekomponenten setzt in der Regel eine kurzfristige Außerbetriebnahme des Hostrechners voraus. In diesem Fall gelten die gleichen Sicherheitsbedingungen, wie unter "UNKONTROLLIERTER STROMAUSFALL" beschrieben. Nach dem Tausch einer defekten Festplatte aus dem RAID-Verbund befinden sich die Aktienregisterserverdaten auf dem Altteil ausschließlich im vollverschlüsselten Zustand. Es ist nach dem aktuellen Stand der Technik nicht vorstellbar, dass von einer getauschten Hardwarekomponente nachträglich - ohne manuelle administrative Entschlüsselung - Kundendaten ausgelesen werden können.

Anlage 2: Zertifikat Unterauftragnehmer Hetzner Online GmbH

FOX Certification

ZERTIFIKAT

FOX Certification GmbH bescheinigt

Hetzner Online GmbH
Industriestraße 25
91710 Gunzenhausen im Geltungsbereich

„Rechenzentrumsinfrastruktur, -betrieb und Serverfertigung an den Standorten in Nürnberg und Falkenstein"

ein Managementsystem nach

ISO/IEC 27001:2013

erfolgreich zu betreiben.

Mit dem Auditbericht vom 10. Oktober 2016 wurde uns der Nachweis erbracht, die Forderungen erfüllt zu haben.

Statement of Applicability (SoA): V 2.2 vom 22. August 2016
Gültigkeit Zertifikat: 11.10.2016 bis 06.10.2019
Re-Zertifizierung: 06.10.2019
Zertifikatsnummer: ZN-2016-04

DAkkS
Deutsche Akkreditierungsstelle
D-ZM-18855-01-00

Stuttgart, 11. Oktober 2016

Geschäftsführung

FOX Certification GmbH Steiermärker Straße 3-5 70469 Stuttgart
This certificate remains property of FOX Certification GmbH and has to be returned on request.

_____	_____
Datum/Unterschrift Auftraggeber	Datum/Unterschrift Auftragnehmer

Alternativ kann diese Vereinbarung vom Auftragnehmer mit fortgeschrittener elektronischer Signatur unterzeichnet werden.
In diesem Fall erhält der Auftraggeber eine Ausfertigung der Vereinbarung als signierte PDF-Datei per E-Mail oder zum Download über den gesicherten Vorstandszugang und zusätzlich mit der Brief-Post eine handschriftlich unterzeichnete Bestätigung der sha1-Checksumme des Signaturzertifikats.

Die Annahme dieser Vereinbarung durch den Auftraggeber kann gegenüber dem Auftragnehmer auch durch Erklärung in Textform per E-Mail oder mit fortgeschrittener elektronischer Signatur erfolgen.