# Vertrag zur Auftragsverarbeitung

zwischen

**Hier Firma und Anschrift eintragen**

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

**VR-Gewinnspargemeinschaft e.V.**

Hannoversche Straße 149

30627 Hannover

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

## Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung.

### § 1 Begriffsbestimmungen

Für in dieser Vereinbarung benutzte Begriffe, für die Art. 4 DSGVO eine Begriffsbestimmung vorsieht, gilt diese gesetzliche Definition in der im Zeitpunkt des Vertragsschlusses geltenden Fassung auch für diesen Vertrag.

### § 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage der Nutzungs- und Teilnahmebedingungen der Social-Voting-Plattform der VR-Gewinnspargemeinschaft e.V., Hannover („Hauptvertrag“). Der Auftragnehmer übernimmt das Hosting und den Betrieb der Social-Voting-Plattform. Zusätzlich kann er den Auftraggeber bei der Durchführung des Wettbewerbs unterstützen, insbesondere im Bewerbungsverfahren, bei der Auswahl der Nominierten, beim Voting, dem E-Mail-Versand an die Abstimmenden und der weiteren Abwicklung einschließlich der Übergabe von ausgelobten Gewinnen (Artikel 6 Absatz 1 Buchstabe b) DSGVO). Dabei kann der Auftragnehmer Zugriff auf personenbezogene Daten erhalten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und, sofern vorhanden, aus der dazugehörigen Leistungsbeschreibung) sowie aus der Anlage 1 zu diesem Vertrag. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen des vorliegenden Vertrages gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht über die Laufzeit des Hauptvertrages hinausgehende Verpflichtungen ergeben. Sich aus diesem Vertrag ergebende Kündigungsrechte bleiben von der vorstehenden Regelung unberührt.

(4) Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

(5) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 3 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers verarbeiten. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern ihm dies rechtlich gestattet ist.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung und Löschung von Daten sowie auf die Einschränkung der Verarbeitung.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer entstehen, bleiben unberührt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten der ebenfalls in Anlage 1 näher spezifizierten betroffenen Personen.

§ 5 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht ohne entsprechende Weisung an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen in Papierform und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 2 aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Abs. 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen, welche in Anlage 2 genauer spezifiziert sind. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung welche Maßnahmen getroffen werden und die Umsetzung der Maßnahmen offen.

Eine Verbesserung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten und der Auftraggeber über wesentliche Veränderungen unverzüglich informiert wird.

(3) Der Auftragnehmer wird einen Datenschutzbeauftragten benennen, sofern er dazu gesetzlich verpflichtet ist.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b DSGVO), über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren und mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen der Mitarbeiter auf Verlangen in geeigneter Weise nachzuweisen.

§ 6 Informationspflichten des Auftragnehmers

(1) Bei Störungen bei den Verarbeitungstätigkeiten, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers oder Verdacht auf sonstige sicherheitsrelevante Vorfälle beim Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde, die für den Auftraggeber relevante Verarbeitungen oder Sachverhalte betreffen. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält, soweit möglich, folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung

c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der betroffenen Daten und zur Minderung möglicher nachteiliger Folgen für die betroffene(n) Person(en), informiert hierüber den Auftraggeber, ersucht ihn um weitere Weisungen und erteilt dem Auftraggeber jederzeit weitere Auskünfte, soweit dessen Daten von einer Verletzung nach Abs. 1 betroffen sind.

(3) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber liegt.

(4) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(5) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(6) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO (soweit diese gesetzlich vorgeschrieben ist) und ggf. bei der vorherigen Konsultation der Datenschutz-Aufsichtsbehörden gem. Art. 36 DSGVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen. Kosten, die dem Auftragnehmer durch seine Unterstützungshandlungen entstehen, sind ihm im angemessenen Umfang zu erstatten.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen

Maßnahmen des Auftragnehmers, sofern möglich, nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Ergebnis der von ihm durchgeführten Kontrollen und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 5 Abs. 4 auf Verlangen nach. Der Auftraggeber vergütet dem Auftragnehmer den angemessenen Aufwand, der ihm im Rahmen der Kontrolle entsteht.

## § 8 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 3 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen Subunternehmerverhältnisse i.S.v. Abs. 1 dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

## § 9 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten des Auftraggebers nach Art. 12–22 sowie 32 und 36 DSGVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

## § 10 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

(2) Der Auftragnehmer stellt den Auftraggeber von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DSGVO auferlegten Pflicht oder wegen der Nichtbeachtung oder Verletzung einer in dieser Vereinbarung festgelegten Pflicht oder einer vom Auftraggeber gesondert erteilten Weisung geltend machen.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn/soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Abs. 5 DSGVO.

(4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 11 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 12 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen in Papierform, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Die Herausgabe- bzw. Vernichtungsverpflichtung betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung zu führen.

(2) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Informationen vertraulich zu behandeln.

§ 13 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass dem Auftragnehmer kein Zurückbehaltungsrecht hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger zusteht.

(2) Änderungen und Ergänzungen dieses Vertrags, die Erklärung einer Kündigung sowie die Abänderung dieser Klausel bedürfen zu ihrer Wirksamkeit der Textform (§ 126 b BGB).

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Hannover.

| | |
|---|---|
| _____ | _____ |
| Datum, Unterschriften Auftraggeber | Datum, Unterschriften Auftragnehmer |

Anlagen

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der Datenkategorien

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

**Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der Datenkategorien**

1. Daten von Mitarbeitern des Auftraggebers

Vorname, Nachname, E-Mail-Adresse, Firma

2. Daten von Einrichtungen und Vereinen (Bewerber)

- Verein, Firma
- Anschrift (Straße, Hausnummer, PLZ, Ort)
- Ansprechpartner (Anrede, Vorname, Nachname, E-Mail, Telefon)
- Bewerbung (Porträt des Bewerbers, Beschreibung des Projektes/Beitrags, ggf. einschließlich Bilder, Videos).

3. Daten von Voting-Teilnehmern (Abstimmende)

E-Mail-Adressen

**Anlage 2a (Seite 1 von 1) – Technische und organisatorische Maßnahmen des Auftragnehmers**

| ***Maßnahmenforderung nach dem Stand der Technik*** | ***Gesetzliche Anforderung*** | ***Umsetzung*** |
|---|---|---|
| Zutrittskontrolle | Unbefugten den Zutritt zu DV-Anlagen verwehren | Sicherheitszonen, Schließanlagen, Schlüsselverwaltung, zentraler Empfang/Anmeldung. |
| Zugangskontrolle | Nutzung von DV-Anlagen durch Unbefugte verhindern | personalisierte Nutzerkennungen, Passwortrichtlinien, Umgang mit IT-Ausstattung |
| Zugriffskontrolle | Gewährleistung der Benutzung einer DV-Anlage und der gespeicherten Daten entsprechend der Berechtigung | Berechtigungskonzepte, Kontrolle, Protokollierungen |
| Weitergabekontrolle/ Übermittlungskontrolle | Übermittlung von Daten darf nur an berechtigte Empfänger geschehen. | Daten-/Verbindungswegverschlüsselung, Authentifizierung |
| Eingabekontrolle/Plausibilitätskontrolle/Transaktionskontrolle | Gewährleistung der Nachverfolgbarkeit von (gewollten und ungewollten) Datenmanipulationen | Plausibilitätsprüfungen, Protokollierungen, Formatbeschränkungen, Nachvollziehbarkeit der Nutzereingaben durch Zeitstempel, Nutzernamen und andere nicht manipulierbare Werte in Systemen, Applikationen und Datenbanken |
| Auftragskontrolle/Vertragskonformitätskontrolle | Sicherstellung der weisungsgemäßen Verarbeitung von Daten im Auftrag | Vor-Ort-Prüfungen, Dokumentensichtung, Vertragsergänzungen |
| Verfügbarkeitskontrolle | Sicherung von Daten gegen zufällige Zerstörung oder Verlust | Back-up-/Recovery-Verfahren, Redundanz, Unterbrechungsfreie Stromversorgung (USV) |
| Datentrennungskontrolle/Mandantentrennungskontrolle | Sicherstellung der Trennung zu unterschiedlichen Zwecken erhobener Daten | Einsatz mandantenfähiger Systeme, Instanziierung in Datenbanken |

# Technische und organisatorische Maßnahmen

Stand: 01.05.2018

## 1. Zutrittskontrolle

Büroräume der new media partners AG:

- Die Büroräume der new media partners AG sind mit Sicherheitsschlössern versehen und alle Schlüsselinhaber werden in einem Schlüsselverzeichnis geführt.
- Besucher werden innerhalb der Räumlichkeiten durch einen Mitarbeiter der new media partners AG begleitet.

IT-Outsourcing / Software-Hosting im Rechenzentrum:

- Der AN unterhält gemietete Netzwerkschränke im verschiedenen Rechenzentren (Anlage 2).
- Die Server-Räume können nur durch berechtigte Personen mit KeyCard betreten werden.
- Die Räume bzw. das Gebäude sind komplett videoüberwacht.
- Alle Zutritte werden auf Video protokolliert.
- Die Schränke der new media partners AG sind durch spezielle Schlüssel abgesichert und können nur durch die Mitarbeiter der nmp AG geöffnet werden (zu Wartungszwecken auch durch Mitarbeiter des Rechenzentrums).
- Nichtberechtigte Personen haben keinen Zutritt zu den Räumlichkeiten des Rechenzentrums.

## 2. Zugangskontrolle

Die new media partners AG sichert die eigenen Systeme und die Systeme des AG durch diverse Schutzmechanismen ab:

- Zugriffe von außen sind durch Firewalls des AN geschützt.
- Die Firewalls des AN filtern durch mehrstufige Kontrollen und Mechanismen den Zugriff von außen.
- Die Wartung der Firewallsysteme erfolgt ausschließlich durch den AN. Weitere Dienstleister sind hiermit nicht beauftragt.
- Der Zugriff von außen (für Smartphones oder Tablets zur Synchronisation von E-Mails/ Kontakten/Kalendern) erfolgt durch eine Verschlüsselung auf dem aktuellen Stand der Technik.
- Der Zugriff innerhalb des Systems auf Internetdienste wird durch Web-Filterung kontrolliert.
- Antivirenprüfung und Contentfilter schützen den User vor Viren und anderer Schadsoftware.
- Die E-Mail-Abholung (falls genutzt) wird durch zweifachen Virenscan und Spamfilterung geschützt.

Die Systeme der Kunden sind untereinander durch Schutzmechanismen isoliert:

- Die Server der Kunden werden durch Einsatz von VLAN-Technik getrennt.
- Die Server der Kunden werden zusätzlich durch Netztrennung auf Ebene von TCP/IP voneinander getrennt.
- Die Systeme werden zusätzlich durch Firewallregeln voneinander abgeschottet.
- Die Systeme sind innerhalb der Maschinen mit Benutzername und Kennwort geschützt.
- Die Kennwörter werden pro Mitarbeiter individuell vergeben.
- Dem AN sind die Kennwörter der Benutzer nicht bekannt.
- Der AN kann die Kennwörter nur zurücksetzen, aber nicht auslesen.

### 3. Zugriffskontrolle

- Der Zugriff auf Systeme der new media partners AG kann ausschließlich durch Eingabe von Benutzername und Kennwort erfolgen.
- Der Benutzer muss sein Kennwort in regelmäßigen Abständen nach den Vorgaben der Passwortrichtlinie erneuern.
- Das interne Berechtigungskonzept stellt sicher, dass jeder Mitarbeiter nur Zugriff auf die Daten erhält, die zur Erfüllung seiner Tätigkeit notwendig sind.
- Administratorzugang haben nur die Leiter der jeweiligen Projektteams und der Leiter der Datenverarbeitung.
- Die Vernichtung von Datenträgern mit personenbezogenen Daten erfolgt gemäß den Vorgaben der DIN 66399.

### 5. Eingabekontrolle

Die Eingabekontrolle wird nur innerhalb der Software-Produkte geregelt. Dies betrifft z. B. Office-Programme, Fibus wie z.B. Lexware, ERP-Systeme wie SAP Business One usw. Der Zugriff auf diese Software-Produkte kann ebenfalls nur mittels Eingabe von Benutzername und Kennwort erfolgen.

### 6. Auftragskontrolle

Es ist sichergestellt, dass personenbezogene Daten die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden. Alle Mitarbeiter der new media partners AG sind gem. § 5 BDSG auf das Datengeheimnis verpflichtet.
In Absprache mit der new media partners AG kann der Auftraggeber Vor-Ort-Kontrollen im Rechenzentrum der new media partners AG durchführen.

Die Auswahl von externen Dienstleistern erfolgt erst nach sorgfältiger Vorab-Prüfung durch die new media partners AG und allen involvierten Fachabteilungen. Eine Auftragserteilung erfolgt ausschließlich nach Abschluss eines Vertrages zur Auftragsdatenverarbeitung nach § 11 BDSG. Für die Auswahl von externen Dienstleistern existiert eine Arbeitsanweisung, die dies sicherstellt.

**Anlage 2b (Seite 3 von 3) – Technische und organisatorische Maßnahmen der new media partners AG**

## 7. Verfügbarkeitskontrolle

- Die Netzwerkschränke des AN sind durch zertifizierte Systeme geschützt. Aktuelle Brandschutzmaßnahmen, Überspannungsschutz und unterbrechungsfreie Stromversorgung mit Dieselaggregaten sind vorhanden.
- Die Räume sind klimatisiert und werden durch Temperatursensoren überwacht (eine Überschreitung der zulässigen Temperaturen wird dem Betreiber signalisiert, dadurch werden weitere Maßnahmen veranlasst).
- Die Systeme sind durch die Zugangskontrolle und diverse Überwachungsmechanismen diebstahlgeschützt.
- Die Systeme des AN sind hochwertige Markensysteme und durch redundante Komponenten größtenteils gegen Ausfall abgesichert, einzelne nicht redundante Komponenten könnten jedoch zu einem Ausfall eines Serversystems führen. Sollten nicht redundante Komponenten einen Ausfall verursachen, so können diese durch immer verfügbare Ersatzgeräte in der Regel innerhalb weniger Stunden wieder instandgesetzt oder durch ein gleichwertiges System wiederhergestellt werden.
- Sollten Kundenserver defekt sein oder durch einen Hardwarefehler zerstört worden sein, müssen die Server von der Datensicherung wiederhergestellt werden. Eine Rücksicherung von Kundenservern aus der Datensicherung kann je nach Menge der Daten bis zu 1-2 Tage dauern.
- Der AN sichert täglich die Server der Kunden; die Datensicherungen werden 30 Tage verfügbar gehalten. Die Datensicherung erfolgt mindestens einmal täglich (in der Regel nachts). Bei Ausfall eines kompletten Servers oder bei Verlust von einzelnen Dateien (unabsichtliches löschen durch AG) können diese Server/Daten in der Regel innerhalb von wenigen Minuten/Stunden wiederhergestellt werden. Die exakte Wiederherstellungsdauer kann nicht festgelegt werden, da diese je nach Menge/Ausmaß unterschiedlich sein kann.
- Die Verfügbarkeit der Serversysteme des AN sind mit 99% festgelegt.

## 8. Trennungsgebot

- Die Zuordnung von personenbezogenen Daten erfolgt innerhalb der jeweiligen Software-Produkte.
- Die Datensätze sind mit Datenfeldern versehen, um die jeweilige Verwendung zu kennzeichnen.
- Durch regelmäßige Unterweisungen zum Datenschutz nach § 4g BDSG sensibilisiert die new media partners AG ihre Mitarbeiter im Umgang mit dem Trennungsgebot.
- Der Einsatz von Testsystemen verhindert eine Nutzung von personenbezogenen Daten zu Testzwecken.

**Anlage 3 (Seite 1 von 1) – Genehmigte Subunternehmer**

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer:

| **Unternehmen mit Namen, Rechtsform, Kontaktdaten und ladungsfähiger Anschrift** | **Umfang und Zweck der Verarbeitung durch den Subunternehmer** |
|---|---|
| new media partners AG<br>Laberstraße 7<br>D-93161 Sinzing<br><br>Florian Kögler, Vorstand<br>www.nmp.ag \|<br>florian.koegler@nmp.ag \|<br>+49-941-307676-17 | Webhosting, Mail-Server-Hosting,<br>IT-Administration, Server-Überwachung |