AUFTRAGSDATENVERARBEITUNG VERTRAG

YOUR EDITING TEAM

Datum: 25/11/2020

1. Die beteiligten Parteien

1.1 Dieser Vertrag über die Sammlung, Speicherung und Nutzung von Dokumenten und Informationen (im Folgenden der "Auftragsdatenverarbeitung") wurde unterzeichnet von und zwischen

a. **Der Verantwortliche:**

Name
Anschrift

[nachfolgend Auftraggeber genannt]

b. **Der Auftrag/Datenverarbeiter**

Your Editing Team
IEC Nummer - ATAPB6736H
NL Cross Roads,
Mumbai 400064
India

[nachfolgend Auftragnehmer genannt]

(im folgenden gemeinsam als "Parteien" und einzeln als "Partei" bezeichnet)

2. DEFINITIONEN

2.1 Begriffe und Ausdrücke mit großen Anfangsbuchstaben, die in diesem Auftragsverarbeitung Vertrag verwendet werden, haben die in der Allgemeinen Datenschutz-Grundverordnung (GDPR 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, nachfolgend "GDPR") festgelegte Bedeutung oder die in diesem Auftragsverarbeitung Vertrag anderweitig definierten Bedeutungen.

2.2 "**Betroffene Personen**" ist die identifizierte oder identifizierbare natürliche Person, auf die sich die persönlichen Daten beziehen.

2.3 "**Unterauftragnehmer**" sind die Unterauftragnehmer der Datenverarbeitung.

2.4 "**Dritte**" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder Organisation mit Ausnahme der betroffenen Person, der Verantwortliche, des Datenverarbeiters, des Datenverarbeiters und der Personen, die unter der direkten Autorität des Datenverarbeiters oder Datenverarbeiters befugt sind, personenbezogene Daten zu verarbeiten.

3. ANWENDUNGSBEREICH

3.1 Diese Auftragsverarbeitungsvertrag betrifft die Verpflichtungen der Parteien in Bezug auf die Verarbeitung personenbezogener Daten.

3.2 Im Rahmen dieses Auftragsdatenverarbeitung Vertrag entscheidet der Datenverarbeiter allein oder gemeinsam mit anderen Parteien, zu welchem Zweck und mit welchen Mitteln personenbezogene Daten verarbeitet werden dürfen. Der Verantwortliche muss den Datenverarbeiter hierüber informieren.

3.3 Dieser Auftragsdatenverarbeitungs Vertrag gilt für alle gegenwärtigen und zukünftigen Lieferungen des Datenverarbeiters im Rahmen der Software-Support- und Lieferbedingungen an alle Unternehmen innerhalb der Unternehmensgruppe des Datenverarbeiters, für die der Datenverarbeiter personenbezogene Daten verarbeitet.

3.4 Dieser Auftragsdatenverarbeitungs Vertrag ergänzt und ist Teil der Software-Support- und Lieferbedingungen. Im Falle von Widersprüchen zwischen diesem Auftragsdatenverarbeitungs Vertrag und den Software-Support- und Lieferbedingungen hat dieser Auftragsdatenverarbeitungs Vertrag Vorrang.

3.5 Ab dem 24. Mai 2018 muss der Datenverarbeiter die EU-Datenschutzrichtlinie (DPD) 1995 und alle Gesetze der Mitgliedsstaaten, die diese Richtlinie umgesetzt haben - einschließlich der britischen Datenschutzbehörde DPA 1998 - einhalten.

3.6 Alle personenbezogenen Daten, die gemäß dieses Auftragsdatenverarbeitung Vertrag verarbeitet

werden, sind Eigentum des für die Verantwortlichen.

4. VORHERIGE SPEZIFISCHE ODER ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG

4.1 Der Datenverarbeiter verarbeitet personenbezogene Daten im Auftrag des für die Datenverarbeitung Verantwortlichen. Der Datenverarbeiter erhält vom Verantwortlichen für die Datenverarbeitung Anweisungen zur Datenverarbeitung.

4.2 Der Verantwortliche weist den Datenverarbeiter an, die personenbezogenen Daten zu verarbeiten, um seine Dienstleistungen gemäß den Software-Support- und Lieferbedingungen zu erbringen.

4.3 Wenn der Datenverarbeiter der Ansicht ist, dass Anweisungen des Verantwortlichen gegen gesetzliche Vorschriften, einschließlich des GDPR oder andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten, verstoßen oder diese verletzen, muss der Datenverarbeiter den Verantwortlichen unverzüglich benachrichtigen.

4.4 Der Datenverarbeiter ist nicht berechtigt, persönliche Daten, Informationen oder anderweitig vom den Verantwortliche für andere Zwecke als die Erfüllung dieser Auftragsdatenverarbeitung zu verwenden. Der Datenverarbeiter darf solche persönlichen Daten nicht für historische, statistische, wissenschaftliche oder ähnliche Zwecke verwenden, weder anonymisiert noch auf andere Weise.

5. GEOGRAPHISCHE EINSCHRÄNKUNGEN

5.1 Dem Datenverarbeiter ist es nicht erlaubt, personenbezogene Daten in Länder außerhalb der EU/EWR zu übertragen, darauf zuzugreifen, sie zu verarbeiten oder anderweitig verfügbar zu machen.

5.2 Der Datenverarbeiter kann personenbezogene Daten an vorab genehmigte Unterauftragnehmer, die in Anhang 1 aufgeführt sind, übertragen, auf sie zugreifen, sie verarbeiten oder anderweitig zur Verfügung stellen. Alle derartigen Vereinbarungen mit vorab genehmigten Unterauftragnehmern außerhalb der EU oder des EWR müssen - vor der Übertragung von Daten - gemäß dem Beschluss der EU-Kommission von 2010/87/EU über den Standard-Mustervertrag für die Übertragung personenbezogener Daten in Länder außerhalb der EU oder des EWR zusätzlich zu einer etwaigen Genehmigung durch lokale Behörden abgeschlossen werden, sofern dies gesetzlich erforderlich ist.

6. VERTRAULICHKEIT

6.1 Die Parteien akzeptieren, sowohl für die Dauer dieses Auftragsdatenverarbeitungs-Vertrags als auch danach, keine vertraulichen Informationen an Dritte weiterzugeben. Diese Verpflichtung zur Nicht-Offenlegung gilt nicht für Informationen, die (a) oder (b) Informationen, die ein Dokument der Partei selbst erstellt hat.

6.2 "Vertrauliche Informationen" sind alle Informationen technischer, geschäftlicher, infrastruktureller oder ähnlicher Art, unabhängig davon, ob diese Informationen dokumentiert wurden, mit Ausnahme von Informationen, die auf andere Weise als durch Verletzung dieser Auftragsdatenverarbeitungs-Vertrag zur Verfügung gestellt werden oder werden, sowie alle personenbezogenen Daten.

6.3 Die Parteien stellen sicher, dass Mitarbeiter und Berater, die vertrauliche Informationen erhalten, verpflichtet sind, eine ähnliche Verpflichtung in Bezug auf vertrauliche Informationen der anderen Partei und die Zusammenarbeit im Allgemeinen in Übereinstimmung mit diesem Auftragsdatenverarbeitungs-Vertrag zu übernehmen.

6.4 Der Datenverarbeiter muss ferner sicherstellen, dass alle Personen mit Zugang zu personenbezogenen Daten, die im Auftrag des Datenverarbeiters verarbeitet werden, mit dieser Auftragsdatenverarbeitungs-Vertrag vertraut sind und den Bestimmungen dieser Auftragsdatenverarbeitungs-Vertrag unterliegen.

7. IT- SICHERHEITSPROTOKOLLEN DES DATENVERARBEITERS

7.1 Der Datenverarbeiter muss die in Anhang I aufgeführten IT-Sicherheitsrichtlinien des Datenverarbeiters einhalten. Der Datenprozessor muss den Verantwortlichen für die Datenverarbeitung jedes Mal schriftlich informieren, wenn eine Änderung an den IT-Sicherheitsrichtlinien des Datenverarbeiters vorgenommen wurde, bevor diese Änderungen in Kraft treten. Auf schriftliche Anfrage muss der Verantwortliche den Datenverarbeiter über den Inhalt solcher Änderungen an den IT-Sicherheitsrichtlinien des Datenverarbeiters informieren.

7.2 Der Datenverarbeiter muss den Kontrollbehörden und dem Verantwortlichen stets den erforderlichen Zugang zu und Einblick in die personenbezogenen Daten, die verarbeitet werden, und die verwendeten Systeme gewähren.

8. PASSENDE TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

8.1 Der Datenverarbeiter muss angemessene und zumutbare technische und organisatorische Maßnahmen ergreifen, um ein Sicherheitsniveau zu gewährleisten, das den Risiken der Datenverarbeitung für die Verarbeitung personenbezogener Daten entspricht, die der für die Datenverarbeitung Verantwortliche im Rahmen dieses Auftragsdatenverarbeitung-Vertrag zur Verfügung stellt, einschließlich der angemessenen Gewährleistung

a) Pseudonymisierung und Verschlüsselung von Personendaten;
b) Kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Robustheit der Verarbeitungssysteme und -dienste, für die der Datenverarbeiter verantwortlich ist;
c) rechtzeitige Wiederherstellung der Verfügbarkeit von und des Zugangs zu Personendaten im Falle eines physischen oder technischen Zwischenfalls;
d) ein Verfahren zur regelmäßigen Prüfung, Beurteilung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitungssicherheit;
e) dass personenbezogene Daten nicht versehentlich oder unrechtmäßig zerstört, verloren oder beeinträchtigt werden und nicht gegen unbefugte Offenlegung, Missbrauch oder auf andere Weise unter Verletzung geltender Gesetze über personenbezogene Daten verarbeitet werden.

8.2 Der Verantwortliche muss das angemessene Niveau der technischen und organisatorischen Maßnahmen festlegen. Bei der Festlegung muss der Datenverarbeiter insbesondere die mit der Verarbeitung verbundenen Risiken berücksichtigen, d.h. die Risiken der zufälligen oder unrechtmäßigen Zerstörung, des Verlusts, der Veränderung, der unberechtigten Weitergabe oder des unberechtigten Zugriffs auf personenbezogene Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

8.3 Der Datenverarbeiter muss auf vorherige schriftliche Anfrage des für die Verarbeitung Verantwortlichen innerhalb angemessener Fristen dem für die Verarbeitung Verantwortlichen ausreichende Informationen zur Verfügung stellen, um zu dokumentieren, dass die oben genannten technischen und organisatorischen Sicherheitsmaßnahmen getroffen wurden.

9. TRANSPARENTE INFORMATION UND KOMMUNIKATION

9.1 Der Datenverarbeiter muss dem für den Verantwortlichen kontinuierlich mit dem vereinbarten Inhalt, der vereinbarten Qualität und Häufigkeit Bericht erstatten. Der Datenverarbeiter muss den Inhaber der Datenverarbeitung unverzüglich über jede Entwicklung informieren, die die gegenwärtige oder zukünftige Fähigkeit oder Möglichkeit des Datenverarbeiters, den Auftragsdatenverarbeitung-Vertrag zu erfüllen, erheblich beeinträchtigen könnte.

9.2 Der Datenverarbeiter ist verpflichtet, den für die Verarbeitung Verantwortlichen unverzüglich zu informieren, wenn der Datenverarbeiter nicht in der Lage ist, die korrekte Verarbeitung der

personenbezogenen Daten des Datenverarbeiters in Übereinstimmung mit dieser Auftragsdatenverarbeitung-Vertrag zu gewährleisten.

10. RECHTE DER BETROFFENEN PERSONEN

10.1 Der Datenverarbeiter muss auf Anfrage des Verantwortliches ohne unangemessene Verspätung dem Verantwortliche alle angefordete Informationen und Unterstützung in Bezug auf die Rechte der betroffenen Person in Bezug auf die folgenden Punkte:

(1) Verarbeitungssicherheit, die dem Datenverarbeiter für jede Verarbeitung personenbezogener Daten bekannt ist, die nicht direkt vom Datenverarbeiter oder einem vorab genehmigten Unterauftragnehmer bereitgestellt wird,
(2) Benachrichtigung der Aufsichtsbehörde über jede Verletzung der Datensicherheit,
(3) Benachrichtigung der betroffenen Person über jede Verletzung der Datensicherheit,
(4) Konsequenzanalyse des Datenschutzes und
(5) Vorläufige Anhörung.

10.2 Der Datenverarbeiter muss auf Anfrage des Datencontrollers und ohne unangemessene Verzögerung dem Datencontroller alle angemessen angeforderten Informationen und Unterstützung in Bezug auf die Rechte der betroffenen Person in Bezug auf die folgenden Punkte zur Verfügung stellen:

(1) Die Informationspflicht bei der Erhebung personenbezogener Daten von der betroffenen Person,
(2) Die Informationspflicht, wenn die Persönlichen Daten nicht bei der betroffenen Person erhoben wurden,
(3) Das Recht der betroffenen Person auf Zugang zu personenbezogenen Daten,
(4) Das Recht auf Berichtigung personenbezogener Daten,
(5) Das Recht, gestrichen zu werden ("das Recht, vergessen zu werden"),
(6) Das Recht auf Beschränkung der Verarbeitung;
(7) die Meldepflicht im Zusammenhang mit der Berichtigung oder Löschung von Persönlichen Daten oder Einschränkungen der Verarbeitungstätigkeit,
(8) Das Recht auf Datenportabilität und
(9) Das Recht, der Verarbeitung personenbezogener Daten zu widersprechen.

11. VERLETZUNG DER DATENSICHERHEIT

11.1 Im Falle eines Verstoßes gegen die Datensicherheit, für den der Datenverarbeiter (oder ein vorab genehmigter Unterauftragnehmer) verantwortlich ist, muss der Datenverarbeiter den für den Verantwortliche so schnell wie praktisch möglich darüber informieren.

Diese Benachrichtigung muss mindestens erfolgen:

11.1.1 eine Beschreibung der Art des Verstoßes gegen die Datensicherheit enthalten, einschließlich, wenn möglich, der Kategorien und der geschätzten Anzahl der betroffenen Personen sowie der Kategorien und der geschätzten Anzahl der betroffenen Registrierungen

personenbezogener Daten,

11.1.2 Geben Sie den Namen und die Kontaktinformationen des Datenschutzbeauftragten (DSB) oder einer anderen Kontaktstelle an, bei der weitere Informationen eingeholt werden können,

11.1.3 Beschreiben Sie die wahrscheinlichen Folgen des Verstoßes gegen die Datensicherheit,

11.1.4 Beschreiben Sie die Maßnahmen, die vom Datenverarbeiter ergriffen werden oder die der Datenverarbeiter vorschlägt, um die Verletzung der Datensicherheit zu behandeln, einschließlich, falls relevant, Maßnahmen zur Begrenzung der möglichen Folgeschäden.

11.2 Der Datenverarbeiter muss alle Datensicherheitsverletzungen dokumentieren, einschließlich der tatsächlichen Umstände der Datensicherheitsverletzung, ihrer Folgen und der getroffenen Abhilfemaßnahmen.

11.3 Diese Dokumentation muss die Aufsichtsbehörde in die Lage versetzen, zu überprüfen, ob der Datenverarbeiter seiner Pflicht nachkommt, über jede Verletzung der Datensicherheit zu informieren.

12. VERWENDUNG VON UNTERAUFTRAGNEHMERN

12.1 Der Datenverarbeiter darf keine Unterauftragnehmer ohne die vorherige schriftliche Zustimmung des Verantwortlichen für die Datenverarbeitung einsetzen.

12.2 Der Verantwortliche hat seine Zustimmung dazu erteilt, dass der Datenverarbeiter die vorab genehmigten Unterauftragnehmer als Unterauftragnehmer einsetzt.

12.3 Der Datenverarbeiter muss den für den Verantwortlichen über alle Pläne zur Vergabe von Unteraufträgen an vorab genehmigte Unterauftragnehmer informieren. Kein Datenverarbeiter darf ohne vorherige schriftliche Zustimmung des Datencontrollers in die Liste der vorab genehmigten Unterauftragnehmer aufgenommen werden.

12.4 Wenn der Datenverarbeiter einen Unterauftragnehmer mit der Durchführung bestimmter Verarbeitungsaktivitäten im Auftrag des Verantwortliches beauftragt, müssen dem Unterauftragnehmer in einer schriftlichen Vereinbarung dieselben Auftragsdatenverarbeitungs-Vertrag auferlegt werden, die in dieser Vereinbarung über die Datenverarbeitung beschrieben sind.

12.5 Wenn der Unterauftragnehmer die Bestimmungen dieser Auftragsdatenverarbeitungs-Vertrag nicht einhält, haftet der Datenverarbeiter für die Handlungen oder Unterlassungen des Unterauftragnehmers zu den gleichen Bedingungen wie für seine eigenen Dienstleistungen.

12.6 Der Datenverarbeiter ist verpflichtet, seine Unterauftragnehmer über die Bestimmungen dieser Auftragsdatenverarbeitungs-Vertrag zu informieren.

13. LIEFERUNG DER PERSONBEZOGENEN DATEN

13.1 Während der Laufzeit dieser Auftragsdateverarbeitungs-Vertrag hat der Verantwortliche vollen Zugang zu allen personenbezogenen Daten, die vom Datenverarbeiter verarbeitet werden.

13.2 Wenn der Inhaber der Daten dies verlangt, ist der Datenverarbeiter verpflichtet, eine Sicherungskopie der persönlichen Daten und zusätzliche Informationen bis zu 3 Monate nach Ablauf oder Beendigung der Auftragsdateverarbeitungs-Vertrag in den Systemen des Datenverarbeiters verfügbar zu halten. Sofern ein solcher Antrag gestellt wurde, kann der für den Verantwortliche bis zum Ablauf dieser dreimonatigen Frist und unabhängig vom Grund für das Auslaufen des Auftragsdateverarbeitungs-Vertrag Zugang zu allen personenbezogenen Daten und zusätzlichen Informationen, die in dieser Sicherungskopie gespeichert sind, beantragen.

13.3 Der Datenverarbeiter darf personenbezogene Daten und Informationen nur an den für die Datenverarbeitung Verantwortlichen und/oder an eine von diesem beauftragte Drittpartei weitergeben.

13.4 Der Datenverarbeiter muss auf schriftliche Anweisung des für den Verantwortlichen Persönliche Daten oder Informationen, die im Rahmen der Auftragsdateverarbeitungs-Vertrag in den Besitz des Datenverarbeiters gelangt sind, löschen.

14. ZUSAMMENARBEIT MIT DER AUFSICHTSBEHÖRDE

14.1 Der Verantwortliche und der Datenverarbeiter sowie gegebenenfalls ihre Vertreter arbeiten auf Verlangen mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

15. KOSTEN

15.1 Alle Kosten, einschließlich der Kosten im Zusammenhang mit der Überarbeitung, Überprüfung und regelmäßigen Durchführung von Maßnahmen nach geltendem Recht und zur Erfüllung der Verpflichtungen des Datenverarbeiters gemäß diesem Auftragsdatenverarbeitungs-Vertrag sind in den Gebühren enthalten, die der Verantwortliche gemäß den Software-Support- und Lieferbedingungen zu entrichten hat. Der Datenverarbeiter hat keinen Anspruch auf separate Gebühren für die Erfüllung solcher Verpflichtungen durch den Datenverarbeiter.

16. DATUM DES INKRAFTTRETEN UND KÜNDIGUNG

16.1 Die Auftragsdatenverarbeitungs-Vertrag tritt an dem Tag in Kraft, an dem die letzte Partei diese Auftragsdatenverarbeitungs-Vertrag unterzeichnet hat.

16.2 Die Auftragsdatenverarbeitungs-Vertrag gilt so lange, wie die Software-Support- und Lieferbedingungen nicht gekündigt oder abgelaufen sind.

16.3 Der für die Datenverarbeitung Verantwortliche ist stets berechtigt, die Datenverarbeitung durch den Datenverarbeiter gemäß diesem Auftragsdatenverarbeitungs-Vertrag auszusetzen.

17. ÄNDERUNGEN IN DER GELTENDEN DATENSCHUTZGESETZGEBUNG

17.1 Wenn eine Änderung der obligatorisch anwendbaren Datenschutzgesetze, die für den Verantwortliche oder den Datenverarbeiter gelten, den Datenverarbeiter verpflichtet

(i) zusätzliche Unterlagen zum Zweck der Einhaltung der Datenschutzvorschriften unterzeichnen oder

(ii) zusätzliche technische und organisatorische Maßnahmen zu den hier aufgeführten ergreifen, oder

(iii) zusätzliche Verpflichtungen zu den hier dargelegten sowie die in

(i) - (iii) oben zusätzliche Kosten oder Risiken für den Datenverarbeiter verursachen, dann vereinbaren die Parteien, in gutem Glauben eine faire Anpassung der anwendbaren Gebühren auszuhandeln.

17.2 Abschnitt 17.1 gilt entsprechend für den Fall

(i) Der Verantwortliche weist den Datenverarbeiter an, Dienstleistungen zu erbringen, die nicht in dieser Auftragsdatenverarbeitungs-Vertrag vorgesehen sind, oder

(ii) Wo zwingende anwendbare Datenschutzgesetze, die für den für die Verarbeitung Verantwortlichen oder den Datenverarbeiter oder die zuständige Aufsichtsbehörde gelten, dem Datenverarbeiter Verpflichtungen auferlegen, die über die hier dargelegten hinausgehen

.

18. ALLGEMEINE BEDINGUNGEN

18.1 Änderungen

Die Bedingungen dieser Auftragsdatenverarbeitungs-Vertrag können nur durch schriftliche Vereinbarung zwischen den Parteien geändert werden.

18.2 **Unabhängige Parteien**

Die Parteien akzeptieren ausdrücklich, dass es sich bei der Beziehung zwischen ihnen um ein kundenunabhängiges Auftragnehmerverhältnis handelt.

18.3 **Informationen**

Die Parteien sind verpflichtet, loyal zueinander zu handeln und sich gegenseitig unverzüglich über alle Änderungen zu informieren, die sich auf diese Auftragsdatenverarbeitungs-Vertrag auswirken können.

18.4 **Höhere Gewalt**

Keine der Parteien ist für Handlungen oder Unterlassungen verantwortlich, soweit diese Handlungen oder Unterlassungen auf Angelegenheiten zurückzuführen sind, die außerhalb der zumutbaren Kontrolle einer Partei liegen, einschließlich, aber nicht beschränkt auf Krieg, Aufstände, höhere Gewalt, Streiks oder andere Arbeitsunterbrechungen (ganz oder teilweise), Störungen des öffentlichen Telenets, Störungen der Internetverbindungen oder ähnliche Vorkommnisse, jedoch nur, wenn diese Partei das Ereignis zum Zeitpunkt der Übernahme der Verpflichtung nicht vorhersehen konnte. Solange ein solches Ereignis eine Partei daran hindert, dieser Verpflichtung nachzukommen, muss dies ausgesetzt werden, bis die Störung nicht mehr besteht.

18.5 **Mitteilungen**

Alle Mitteilungen im Zusammenhang mit dieser Auftragsdatenverarbeitungs-Vertrag müssen der anderen Partei entweder persönlich oder per Einschreiben zugestellt werden.

18.6 **Abtretung**

Der Verantwortliche kann seine Rechte und Pflichten aus dieser Auftragsdatenverarbeitungs-Vertrag ganz oder teilweise an eine dritte Partei abtreten. Der Datenverarbeiter darf seine Rechte und Pflichten aus dieser Datenverarbeitungsvereinbarung nicht ohne vorherige schriftliche Zustimmung des für die Datenverarbeitung Verantwortlichen an einen Dritten abtreten.

18.7 **Ungültige Bedingung** Wenn eine Bedingung oder eine Bestimmung in dieser Auftragsdatenverarbeitungs-Vertrag ungültig ist, bedeutet diese Ungültigkeit nicht, dass der übrige Teil dieses Auftragsdatenverarbeitungs-Vertrags ungültig ist. Wird das anwendbare Recht in Bezug auf personenbezogene Daten nach dem Datum des Inkrafttretens dieses Auftragsdatenverarbeitungs-Vertrag geändert, ist der Verantwortliche verpflichtet, solche Änderungen dieses Auftragsdatenverarbeitungs-Vertrag zu akzeptieren.

18.8 **Geltendes Recht**

Diese Auftragsdatenverarbeitungs-Vertrag unterliegt indischem Recht mit dem Stadtgericht von Mumbai als Gerichtsstand. Das indische Übereinkommen über Verträge für Ihr Your Editing Team gilt nicht für die Auftragsdatenverarbeitungs-Vertrag.

UNTERSCHRIFT

_____ _____

Auftraggeber/Data Controller Your Editing Team (Datenverarbeiter)

Anhang I - IT-Sicherheitsrichtlinien für Datenprozessoren

1 Der Zugang zu Personendaten ist auf Personen beschränkt, die ein materielles Bedürfnis nach Zugang zu Personendaten haben. Personenbezogene Daten werden nur auf der Grundlage des "need to know"-Grundsatzes zugänglich gemacht.

2 Mitarbeiter, die mit Persönlichen Daten umgehen, werden instruiert und geschult, was sie mit Persönlichen Daten zu tun haben und wie sie Persönliche Daten schützen können.

3 Es dürfen möglichst wenige Personen Zugang zu Persönlichen Daten haben, wobei der Vorgang gebührend zu berücksichtigen ist. Es muss jedoch eine ausreichende Anzahl von Mitarbeitern vorhanden sein, um den Betrieb der betreffenden Aufgaben im Falle von Krankheit, Urlaub, Personalvertretung usw. sicherzustellen. Persönliche Daten werden nur auf einer "Need to know"-Basis zugänglich gemacht.

4 Personenbezogene Daten auf Papier - z.B. in Kartons und Ordnern - werden verschlossen und verschlossen gehalten, wenn sie nicht gebraucht werden.

5 Wenn Dokumente (Papiere, Diagramme usw.) weggeworfen werden, werden Aktenvernichtung und andere Maßnahmen eingesetzt, um den unbefugten Zugriff auf Persönliche Daten zu verhindern.

6 Wir verwenden Zugangscodes für den Zugriff auf PCs und andere elektronische Geräte mit Persönlichen Daten. Nur diejenigen, die Zugang haben müssen, erhalten einen Zugangscode und dann auch nur für die Systeme, die sie benutzen müssen. Diejenigen, die ein Passwort haben, dürfen den Code nicht anderen überlassen oder ihn so hinterlassen, dass andere ihn sehen können. Die Überprüfung der zugewiesenen Codes muss mindestens einmal alle sechs Monate erfolgen.

7 Erfolglose Versuche, mit persönlichen Daten auf IT-Systeme zuzugreifen, werden erkannt und protokolliert. Wird eine bestimmte Anzahl von aufeinanderfolgenden abgelehnten Zugriffsversuchen festgestellt, müssen weitere Versuche blockiert werden.

8 Wir haben eine verantwortliche Person ernannt, die solche unzugänglichen Zugriffsversuche überwacht. In Anbetracht der technologischen Entwicklung steht Software zur Verfügung, mit der geklärt werden kann, wer versucht hat, Zugang zu Personendaten zu erhalten.

9 Wenn persönliche Daten auf einem USB-Schlüssel gespeichert sind, müssen diese geschützt werden, z.B. durch die Verwendung eines Passworts und eines Verschlüsselungsschlüssels. Andernfalls muss der USB-Schlüssel in einer verschlossenen Schublade oder einem Schrank aufbewahrt werden. Ähnliche Anforderungen gelten für die Speicherung von Personendaten auf anderen tragbaren Datenträgern.

10 PCs, die mit dem Internet verbunden sind, müssen über eine aktualisierte Firewall und Virenkontrolle verfügen. Beim Anschluss an WiFi für den freien Zugang gewährleisten wir angemessene Sicherheitsmaßnahmen unter Berücksichtigung des aktuellen Stands der technischen Entwicklung im IT-Bereich.

11 Werden sensible personenbezogene Daten oder Sozialversicherungsnummern per E-Mail über das Internet verschickt, müssen solche E-Mails verschlüsselt werden. Wenn Sie persönliche Daten per E-Mail an uns senden, beachten Sie bitte, dass das Senden an uns nicht sicher ist, wenn Ihre E-Mails nicht verschlüsselt sind.

12 Bei der Reparatur und Wartung von Datengeräten, die Persönliche Daten enthalten, und wenn Datenträger verkauft oder entsorgt werden sollen, ergreifen wir die notwendigen Massnahmen, um zu verhindern, dass Informationen an Dritte weitergegeben werden.

13 In den Fällen, in denen ein Computer zur Reparatur eingereicht wird und persönliche Daten auf diesem Computer gespeichert werden, legen wir mehrere Zugangscodes für verschiedene Abschnitte der persönlichen Daten fest. Zum Beispiel muss eine Reparaturwerkstatt nicht in der Lage sein, auf persönliche Daten zuzugreifen, die sich möglicherweise auf dem Computer befinden. Ein solches Multi-Code-Schema kann das Risiko des Missbrauchs von Personendaten verringern, aber nicht ausschalten. Darüber hinaus sollte durch Vereinbarung und Überprüfung sichergestellt werden, dass die Werkstätten keinen unberechtigten Zugriff auf personenbezogene Daten haben, z.B. durch die Verwendung von Vertraulichkeitserklärungen.

14 Wenn wir einen externen Datenverarbeitungsagenten für die Verarbeitung personenbezogener Daten einsetzen, wird eine schriftliche Datenverarbeitungsvereinbarung zwischen uns und dem Unterdatenverarbeiter unterzeichnet. Dies gilt zum Beispiel, wenn wir ein externes Dokumentenarchiv verwenden oder wenn bei der Verarbeitung personenbezogener Daten - einschließlich der Kommunikation mit dem Kunden - Cloud-Systeme eingesetzt werden. Ebenso wird immer dann eine schriftliche Vereinbarung zwischen uns und unserem Kunden geschlossen, wenn wir als Datenverarbeiter auftreten. Auftragsdatenverarbeitungs-Vertrag sind auch elektronisch verfügbar.

15 Wir haben interne Vorschriften zur Informationssicherheit. Wir haben interne Vorschriften zur Informationssicherheit erlassen, die Anweisungen und Maßnahmen enthalten, die personenbezogene Daten vor Zerstörung, Verlust oder Änderung, vor unbefugter Offenlegung und vor unbefugtem Zugriff oder unbefugter Kenntnisnahme schützen. Wir werden dafür sorgen, dass die gesammelten Persönlichen Daten mit Sorgfalt behandelt und gemäß den geltenden Sicherheitsstandards geschützt werden. Wir verfügen über strenge Sicherheitsverfahren für das Sammeln, Speichern und Übertragen Persönlicher Daten, um unbefugten Zugriff und die Einhaltung der geltenden Gesetze zu verhindern.

16 Wir haben die erforderlichen technischen und organisatorischen Sicherheitsvorkehrungen getroffen, um Ihre persönlichen Daten vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust oder Änderung sowie vor unbefugter Offenlegung, Missbrauch oder anderen Handlungen, die gegen geltendes Recht verstoßen, zu schützen.

17 Die Systeme befinden sich auf Servern in gesicherten Räumlichkeiten.

18 Wir verwenden Industriestandards wie Firewalls und Authentifizierungsschutz, um Ihre persönlichen Daten zu schützen.

19 Alle zwischen Client (Browser und Webanwendung) und Server(n) übertragenen Daten werden nach dem HTTPS-Protokoll verschlüsselt.

20 Alle Einrichtungen sind verschlossen, und nur Mitarbeiter, die eine Vertraulichkeitserklärung unterzeichnet haben, haben Zugang zu den Einrichtungen. Nach dem Ende der normalen Arbeitszeiten werden die Einrichtungen verschlossen. Der Zugang zu den Einrichtungen erfolgt immer unter der Aufsicht eines Mitarbeiters.

21 Jeder Zutritt zu unseren Räumlichkeiten wird mit einem elektronischen Schlüssel protokolliert oder in das Gästebuch eingetragen.

22 Wir machen jede Nacht ein Backup aller Datenbanken und Dateien auf gemeinsam genutzten Laufwerken. Das Backup wird auf einem internen Server gespeichert, teilweise in einem externen Datenzentrum.

23 Wir erstellen die folgenden Arten von Backups:
a) Rollende Sicherung. Bei dieser Methode wird täglich ein Backup aller Datei- und Datenaktualisierungen durchgeführt und ein Backup aller neuen Daten erstellt. Dadurch wird eine Historie der Änderungen erstellt, so dass die Fähigkeit zur Wiederherstellung verlorener Daten erhöht wird.
b) Sicherungs-Klon. Diese Sicherungsstrategie erstellt eine perfekte Kopie von jedem Gerät im Netzwerk.
c) Offsite-Backup. Diese Sicherung schützt vor Datenverlust, wenn die Sicherung vor Ort gespeichert wird. Alle Daten und Dateien werden gesichert und die Datensicherung außerhalb des Standorts aufbewahrt.

24 Alle Backup-Daten und -Dateien werden in Abständen von 30 Tagen überschrieben. Es ist technisch nicht möglich, einzelne Dateien auf einem Backup vollständig zu löschen, bevor ein solches Überschreiben erfolgt. Wenn Sie also von uns die Löschung persönlicher Daten verlangen, werden diese persönlichen Daten in der Live-Umgebung gelöscht, bleiben aber auf dem Backup, bis das spezifische Backup nach 30 Tagen überschrieben wird. Wir haben jedoch interne Prozesse und Verfahren eingeführt, um sicherzustellen, dass Persönliche Daten nicht wieder als Live-Daten eingeführt werden, indem Daten und Dateien von einem Backup neu geladen werden, da Persönliche Daten gemäß dem "Recht auf Vergessen" gelöscht wurden.