mula.

Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO

Auftragnehmer (Auftragsverarbeiter):

Go Mula GmbH
Colditzstraße 34-36
12099 Berlin
Deutschland

Auftraggeber (Verantwortlicher):

xxxx
xxxx
xxxx
xxxx

1. Gegenstand und Dauer der Vereinbarung

1.1. Der Auftragnehmer stellt dem Auftraggeber eine Plattform zum Merchandise Management zur Verfügung. Über diese Plattform hat der Auftraggeber insbesondere die Möglichkeit, Merchandise-Artikel zu gestalten und den Versand der Artikel zu verwalten. Der Auftragnehmer verarbeitet dabei personenbezogene Daten des Auftraggebers („Auftraggeber-Daten“) auf Grundlage dieses Vertrages. Der Auftragnehmer verarbeitet die personenbezogenen Daten während der Dauer des Hauptvertrages im Auftrag und nur nach Weisung des Auftraggebers.

1.2. Einzelheiten des Leistungsumfangs ergeben sich aus dem Hauptvertrag.

1.3. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Übermittlung personenbezogener Auftraggeber-Daten in ein Land außerhalb der EU/des EWR („Drittland“) darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

1.4. Der Vertrag beginnt mit Unterzeichnung des Hauptvertrages und wird auf unbestimmte Zeit geschlossen. Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

2.1. Art und Zweck der Verarbeitung:
Der Auftraggeber hat über die Plattform die Möglichkeit, personenbezogene Daten von Beschäftigten oder sonstigen Personen hochzuladen und sodann für das Design und/oder die Versandverwaltung der Merchandise-Artikel zu verwenden. Dafür erhebt und speichert

der Auftragnehmer die personenbezogenen Daten und legt sie auf Weisung des Auftraggebers an externe Stellen (z.B. Versanddienstleister) offen. Zweck der Datenverarbeitung ist die Bereitstellung der Plattform sowie die Erfüllung der Leistungen gemäß des Hauptvertrages.

Optional kann der Auftraggeber zur Übertragung der personenbezogenen Beschäftigtendaten auch ein bestehendes System (z.B. HR-System) über eine API an die Plattform anbinden.

Auf Wunsch bietet der Auftragnehmer zudem die Möglichkeit, einen Webshop einzurichten und zu betreiben, über den der Auftraggeber seine Merchandise-Artikel zum Kauf anbieten kann. Der Auftraggeber bestimmt dabei im Rahmen der bereitgestellten Möglichkeiten über die Gestaltung des Shops sowie die angebundenen Zahlungs- und Versanddienstleister.

2.2. Art der personenbezogenen Daten:
Der Auftraggeber bestimmt eigenständig, welche personenbezogenen Auftraggeber-Daten im Rahmen des Auftrags verarbeitet werden. In der Regel verarbeitet der Auftragnehmer zur Erfüllung der Leistungen die folgenden personenbezogenen Auftraggeber-Daten:

- Kontaktdaten (Name, Lieferadresse, Telefon, E-Mail);
- Inhaltsdaten zum Druck auf die Produkte (z.B. Fotos, sonstige bereitgestellte Informationen);
- Daten für den automatisierten Versand (z.B. Geburtstag, Jubiläen, sonstige Anlässe);
- Technische Protokolldaten / Logdaten.

Sofern der Auftragnehmer im Rahmen des Vertrages einen Webshop betreibt, werden regelmäßig die folgenden zusätzlichen Informationen verarbeitet:

- Informationen zur Bestellung (z.B. Inhalt, Zeitpunkt, gewählter Versanddienst);
- Informationen zu etwaigen Credits, mit denen Beschäftigte des Kunden Artikel erwerben können;
- Zahlungsinformationen (z.B. Zahlungsart, pseudonymisierte Zahlungsdaten, Zeitpunkt der Zahlung).

2.3. Kategorien betroffener Personen:
Sämtliche Personen, deren personenbezogene Daten im Rahmen der Leistungen vom Auftraggeber bereitgestellt bzw. hochgeladen werden. In der Regel betrifft dies

- Beschäftigte des Auftraggebers
- Interessent:innen und Endkund:innen des Auftraggebers

3. Rechte und Pflichten des Auftraggebers

3.1. Für die Beurteilung der Rechtmäßigkeit der Verarbeitung 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.

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

3.3. 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.

4. Weisungen

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

4.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

4.3. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

5. Pflichten des Auftragnehmers

5.1. Soweit sich eine betroffene Person in Wahrnehmung ihrer Rechte aus Kapitel 3 DSGVO (Art. 12 bis 23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32 bis 37 BDSG) unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer unterstützt den Auftraggeber auf zumutbare Weise mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung solcher Anträge auf Wahrnehmung der in Kapitel 3 DSGVO benannten Rechte der betroffenen Person nachzukommen.

5.2. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

5.3. Der Auftragnehmer verpflichtet sich, bei der vertragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

5.4. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet.

5.5. Der Verantwortliche und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde zusammen. Bei Kontrolle des Verantwortlichen durch eine Aufsichtsbehörde hat der Auftragnehmer diesen bestmöglich zu unterstützen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

6.1. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

6.2. Wenn dem Auftragnehmer hinsichtlich der verarbeiteten Auftraggeber-Daten eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO bekannt wird („Datenschutzvorfall“), meldet er dies dem Verantwortlichen unverzüglich und unterstützt den Auftraggeber bei etwaigen Pflichten aus den Art. 33, 34 DSGVO.

7. Unterauftragsverhältnisse mit Subunternehmern

7.1. Der Auftragnehmer darf Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern (Subunternehmer) begründen.

7.2. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen innerhalb von zwei Wochen Einspruch zu erheben. Sofern der Auftraggeber innerhalb von zwei Wochen ab Mitteilung über die Änderung keine begründeten Einwände erhebt, gilt diese als durch den Auftraggeber genehmigt. Der Auftragnehmer weist den Auftraggeber bei Beginn der Frist auf diese Bedeutung seines Verhaltens hin. Im Fall eines Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtige Änderung für den Auftragnehmer nicht zumutbar ist – die Leistung gegenüber dem Auftraggeber innerhalb von zwei Wochen nach Zugang des Einspruchs einstellen und den Hauptvertrag fristlos und mit sofortiger Wirkung kündigen.

7.3. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

7.4. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Der Auftragnehmer hat den Auftraggeber dazu vor Aufnahme der Tätigkeiten im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zu verpflichten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

7.5. Zum Zeitpunkt der Beauftragung beschäftigt der Auftragnehmer die folgenden Subunternehmer:

- **Deutsche Post AG, Charles-de-Gaulle-Straße 20, 53113 Bonn, Deutschland**
    - Auslösung der Sendungen über die Plattform, Übersicht der Sendungen, Sendungsverfolgung

- **Amazon Web Services EMEA, SARL, B 186.284, 38 Avenue John F. Kennedy, L-1855 Luxemburg**
    - RDS-Datenbankspeicher für Produktionsdatenbank und Backups

- **Google Cloud EMEA Limited, 368047, 70 Sir John Rogerson's Quay, Dublin 2, Irland**
    - Speicherung von Backups, Datensnapshots und eingereichten Sammellieferungslisten.

- **Mailjet SAS (Global HQ), 4 rue Jules Lefebvre, 75009 Paris, France**
    - Transaktionsbezogene Email Mitteilungen

- **Stripe Payments Europe, Limited (SPEL), 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland**
    - (Optional) Verarbeitung von persönlichen und Zahlungsdaten zur Abwicklung von Shop-Zahlungen (Stripe Connect)

- **allbranded GmbH, Stahltwiete 21a, 22761 Hamburg, Deutschland (Muttergesellschaft)**
    - Unterstützung beim Betrieb der Plattform (insb. Bereitstellung von IT-Systemen, Unterstützung bei der Abwicklung von Bestellungen)

8. Technische und organisatorische Maßnahmen

8.1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Der Auftragnehmer ergreift dazu alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen. Diese Maßnahmen schließen insbesondere die Fähigkeit ein, die Vertraulichkeit, die Integrität, die Verfügbarkeit sowie der Belastbarkeit der Systeme auf Dauer sicherzustellen und die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

8.2. Der Auftragnehmer garantiert, dass er vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 1** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen implementiert, während der Dauer der Verarbeitung aufrechterhält und wenn erforderlich dem Stand der Technik und dem Risiko der Verarbeitung anpassen wird.

8.3. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

8.4. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Kontrollrechte des Auftraggebers

9.1 Der Auftragnehmer räumt dem Auftraggeber ein Kontrollrecht zur Prüfung der Datenverarbeitung sowie Einhaltung dieses Vertrags bzw. des jeweiligen Projektauftrags ein.

Insbesondere stellt der Auftragnehmer dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht die Durchführung von Überprüfungen einschließlich Inspektionen. Die Kontrollhandlungen können ebenfalls durch einen zur Geheimhaltung verpflichteten Dritten vorgenommen werden, sofern es sich bei dem Dritten um keinen Konkurrenten des Auftragnehmers handelt.

9.2 Die Parteien sind sich einig, dass der Auftraggeber eine Überprüfung nach Ziffer 9.1 durchführt, indem er den Auftragnehmer anweist, nach seiner Wahl ein geeignetes Testat, einen Bericht oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Datenschutzauditor oder Qualitätsauditor) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit – z.B. nach ISO 27001) vorzulegen. In begründeten Ausnahmen kann der Auftraggeber eigenständige Inspektionen durchführen.

9.3 Der Auftragnehmer verpflichtet sich, die Durchführung der Kontrollen zu unterstützen. Dies beinhaltet die Gewährung sämtlicher benötigter Zugangs-, Auskunfts- und Einsichtsrechte. Gleiches gilt für öffentliche Kontrollen durch die zuständige Aufsichtsbehörde gemäß den anwendbaren Datenschutzvorschriften.

9.4 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

10. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

10.1. Der Auftragnehmer ist verpflichtet, die personenbezogenen Daten nach Abschluss der Arbeiten bzw. bei Beendigung/Kündigung des Vertrages - nach den Vorgaben des Auftraggebers - vollständig datenschutzgerecht zu löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Auftraggeber zurückzugeben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

10.2. Dokumentationen und Protokolle, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Schlussbestimmungen

11.1. Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt. Vertragsänderungen oder Ergänzungen sind schriftlich festzuhalten.

11.2. Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

Unterschriften

Berlin, xx.xx.xxxx	Berlin,xx.xx.xxxx
Go Mula GmbH	xxxxxxxx
_____	_____

Anlagen:

- Anlage 1: Technische und organisatorische Maßnahmen

Anlage 1: Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Zutrittskontrolle
Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Beispiele für mögliche Vorkehrungen

- Eingangstüren werden stets verschlossen gehalten.
- Besucher/Externe werden begleitet bzw. abgeholt und stets beaufsichtigt.
- Videoüberwachung mit Aufzeichnung an der Eingangstür
- Schlüssel
- Sicherheitsdienst und/oder Sicherheitspersonal am Eingang
- Einzelne IT-Systeme werden in externen Rechenzentren (Hosting) und bei externen Diensten betrieben (Software-as-a-service). Dort gewährleistet der jeweilige Anbieter die Zutrittskontrolle.

Zugangskontrolle/Verschlüsselung
Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Beispiele für mögliche Vorkehrungen

- Zugang zu extern gehosteten/betriebenen IT-Systemen ist besonders gesichert (Verschlüsselung)
- Zugang zu IT-Systemen nur mit Benutzerkennung und individuellem Passwort möglich
- Zugangsberechtigungen werden dokumentiert.
- Passwortrichtlinie wird auf der mula platform durchgesetzt.
- IT-Systeme werden bei wiederholt erfolglosem Anmeldeversuch automatisch gesperrt.
- Funktionale Zuordnung einzelner Endgeräte und Protokollierung der Systemnutzung
- Mobile Datenträger sind verschlüsselt (Hardwareverschlüsselung).
- Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit
- Zwei-Faktor-Identifizierung

Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Beispiele für mögliche Vorkehrungen

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer (in einem schriftlichen Berechtigungskonzept dokumentiert), zentrale Verwaltung und Steuerung
- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.
- Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.
- Aufzeichnung von Zugriffen auf das IT-System

Trennungskontrolle/Zweckbindungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Beispiele für mögliche Vorkehrungen

- Softwareseitige Mandantentrennung
- Trennung von Produktiv- und Testsystemen (in getrennten Datenbanken)

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

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:

Beispiele für mögliche Vorkehrungen

- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung).
- Mitbringen und verwenden privater Datenträger ist untersagt. Es dürfen nur verschlüsselte betriebliche Datenträger genutzt werden.
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN.

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

Beispiele für mögliche Vorkehrungen

- automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung
- Protokollierung gescheiterter Zugriffsversuche
- Protokollierung der Aktivitäten des Systemverwalters und sämtlicher Benutzer
- Protokollierung aller Aktivitäten auf dem Server
- Sicherung der Protokolldaten gegen Verlust oder Veränderung
- Dokumentation der Eingabeprogramme

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

Beispiele für mögliche Vorkehrungen

- Datensicherheitskonzept
- Versionierte Daten- und Systembackups nach Backup-Plan (täglich/ wöchentlich)
- Backup-Rechenzentrum
- Schadsoftwareschutz
- Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt.
- Berichtsverfahren und Notfallplan
- Unterbrechungsfreie Stromversorgung

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO, Art. 25 Abs. 1 DSGVO)

Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden

Beispiele für mögliche Vorkehrungen

- Auftragnehmer werden sorgfältig ausgesucht.
- Klare und unzweifelhafte vertragliche Regelungen zur Datenverarbeitung
- Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten.

Datenschutz-Management
Maßnahmen, die eine Steuerung der Datenschutzprozesse ermöglichen und die Einhaltung der datenschutzrechtlichen Vorgaben nachweisbar sicherstellen:

Beispiele für mögliche Vorkehrungen

- Es wurde eine fachkundige Person zum Datenschutzbeauftragten benannt.
-
- Beschäftigte werden regelmäßig im Datenschutz geschult und sensibilisiert und sind über die Vertraulichkeit von Daten belehrt.
- Beschäftigte haben Verschwiegenheitsklauseln in ihren Arbeitsverträgen