Aufnahmeantrag

Sepa-Lastschriftmandat

Montessori e.V. Feuerbach
Feuerbacher Talstr. 215
70469 Stuttgart

Gläubiger-Identifikationsnummer :	DE66 ZZZ0 0001 4856 94
Mandatsreferenz:	Mitgliedschaft

Bitte ankreuzen: Jahresbeitrag ☐ Ordentliche Mitgliedschaft 75,00 € ☐ Fördermitgliedschaft: 30,00 €

Vorname und Name Erziehungsberechtigte/r:	
Anschrift Erziehungsberechtigte/r:	
eMailadresse Erziehungsberechtigte/r:	
Bei Familienmitgliedschaft	
Name des Kindes:	
Geburtsdatum des Kindes:	

☐ Hiermit willige ich in die zweckbezogene Verarbeitung meiner Daten ein.

Erteilung einer Einzugsermächtigung und eines SEPA- Lastschriftmandats

Der Beitrag wird zum 01.07. eines jeden Jahres eingezogen.
Bei neuen Mitgliedern unterjährig wird der Beitrag mit dem Eintritt erhoben.

Ich ermächtige den Montessori e.V. Feuerbach, Zahlungen von meinem Konto mittels Lastschrift einzuziehen. Zugleich weise ich mein Kreditinstitut an, die von der den Montessori e.V. Feuerbach auf mein Konto gezogenen Lastschriften einzulösen.
Hinweis: Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen.

Name des Kreditinstituts:	
BIC:	
IBAN:	
Datum, Ort, Unterschrift des/der Kontoinhabers/in	

Bitte beachten Sie die geltenden Datenschutzinformationen

DATENSCHUTZRICHTLINIE
nach EU-Datenschutz-Grundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG)

0. Vorwort
Jede für das Unternehmen tätige Person hat zumindest gelegentlich mit personenbezogenen Daten zu tun. Es ist daher notwendig, sich mit den wichtigsten Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) ver¬traut zu machen. Der Schutz personenbezogener Daten nach der DSGVO und dem BDSG erstreckt sich auf alle Arten von Datenbeständen mit personenbezogenen Daten (von Beschäftigten, Kunden, Interessenten, Lieferanten sowie Vertriebs- und Kooperationspartner) und auf die Verfahren, mit denen solche Daten verarbeitet werden. Im Folgenden werden deshalb die wichtigsten Abschnitte der gesetzlichen Regelungen gem. DSGVO und BDSG dargestellt, die bei der täglichen Arbeit von Bedeutung sind.

Verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch die risikobewusste Nutzung von IT-Systemen und Anwendungen sind die zentralen Zielsetzungen. Fehlverhalten kann zu großen materiellen und immateriellen Schäden mit teilweise beträchtlichen negativen Auswirkungen für das Unternehmen führen.

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie über unseren Datenschutzbeauftragten.

1. Grundlagen
Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein **Grundrecht**. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das **Recht auf Schutz** der sie betreffenden **personenbezogenen Daten.**

Die gesetzliche Grundlage für den Datenschutz ist die **EU-Datenschutz-Grundverordnung (DSGVO)** (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016) mit der der im Amtsblatt der Europäischen Union am 4. Mai 2016 unter L 119/1 veröffentlichten, im Amtsblatt der Europäischen Union am 22. November 2016 unter L 314/72 und am 23.05.2018 unter L 127/2 berichtigten amtlichen Fassung und das **Bundesdatenschutzgesetz (BDSG)** (Datenschutz-Anpassungs-und-Umsetzungsgesetz EU-DSAnpUG-EU) vom 30 Juni 2017 (BGBl I, S. 2097).

2. Sachlicher Anwendungsbereich
Die Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

3. Örtlicher Anwendungsbereich
Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Europäischen Union erfolgt, unabhängig davon, ob die Verarbeitung in der Europäischen Union stattfindet.

Darüber hinaus findet die DSGVO auch dann Anwendung, wenn der Verantwortliche oder Auftragsverarbeiter nicht in der Europäischen Union niedergelassen ist. Hierfür ist es erforderlich, dass es sich um die Verarbeitung personenbezogener Daten von betroffenen Personen handelt, die sich in der Europäischen Union befinden. Darüber hinaus muss der nicht in der Europäischen Union niedergelassene Verantwortliche oder Auftragsverarbeiter Waren oder Dienstleistungen in der Europäischen Union anbieten oder das Verhalten der betroffenen Personen beobachten.

4. Begrifflichkeiten
„Personenbezogene Daten" sind nach Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen (Beschäftigten, Kunden, Interessenten, Lieferanten sowie Vertriebs- und Kooperationspartner); als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Beispiele hierfür sind: Adresse, Telefonnummer, Geburtsdatum, Foto, Arbeitgeber, Gehalt, Vermögen, Besitz, Urlaubsplanung, Arbeitsverhalten und Arbeitsergebnisse. Auch Daten ohne direkten Personenbezug (z. B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen Bezug genommen werden kann (z.B. Personalnummer, PC-Benutzerkennung, maschinenbezogene Nutzungszeiten bei nur einem infrage kommenden Benutzer).

„Verarbeitung" nach Art. 4 Abs. 2 DSGVO meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„Besondere Kategorien personenbezogener Daten" nach Art. 9 DSGVO, auch „sensible Daten" genannt, sind solche Daten aus denen sich die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit ergeben. Darüber hinaus zählen genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung ebenfalls zu den besonderen Kategorien personenbezogener Daten. Hier gelten besondere Vorschriften, da diese Daten besonders schutzwürdig sind.

5. Grundsätze der Verarbeitung
Personenbezogene Daten müssen nach Art. 5 Abs. 1 lit. a DSGVO auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz").

Darüber hinaus müssen personenbezogene Daten nach Art. 5 Abs. 1 lit. f DSGVO in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bedarf einer Rechtsgrundlage. Bei der Erhebung der Daten ist außerdem der Zweck, für den die Daten verarbeitet werden, konkret festzulegen.

Die wesentlichen Zulässigkeitsvoraussetzungen für die Datenverarbeitung gem. DSGVO sind:
- zur Erfüllung eines Vertrages oder einer vorvertraglichen Maßnahme
- Einwilligung der betroffenen Person, die freiwillig erfolgt und nachweisbar ist. Ein Vertrag darf nicht zusätzlich von einer Einwilligung abhängig gemacht werden (Kopplungsverbot)
- zur Erfüllung einer rechtlichen Verpflichtung
- zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen der betroffenen Person überwiegen
- zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person
- bei Datenverarbeitungen zu neuen Zwecken, sofern diese mit dem Ursprungszweck kompatibel sind

Weitere Zulässigkeitsvoraussetzungen durch das BDSG:
- Datenverarbeitung im Beschäftigungsverhältnis
- Videoüberwachung
- Datenübermittlung an Auskunfteien
- Scoring

Bei der Datenverarbeitung ist zu beachten, dass die personenbezogenen Daten sachlich richtig sein müssen und nur so lange gespeichert werden dürfen, wie es der genannte Zweck erfordert. Unrichtige oder unvollständige Daten sind zu löschen oder zu berichtigen. Nur in gesetzlich bestimmten Fällen oder mit Einwilligung des Betroffenen ist eine anderweitige Verarbeitung zulässig.

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten nach Art. 29 DSGVO **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Recht der Europäischen Union oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Bei der Beurteilung des angemessenen Schutzniveaus nach Art. 32 Abs. 2 DSGVO sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung - insbesondere durch **Vernichtung, Verlust oder Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden - verbunden sind.

Im Falle einer **Verletzung** des Schutzes personenbezogener Daten meldet der Verantwortliche nach Art. 33 Abs. 1 Abs. 1 DSGVO unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

6. Datensicherheit durch entsprechende technische und organisatorische Maßnahmen
Die DSGVO verlangt die Umsetzung von angemessenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies schließt unter anderem folgende Maßnahmen ein:

Vertraulichkeit
- **Zutrittskontrolle:** kein unbefugter Zutritt zu Datenverarbeitungsanlagen z. B. durch Sicherheitsschlösser, Transponderschließanlagen, elektrische Türschließer, Sicherheitsdienst, Alarmanlagen, Videoüberwachung
- **Zugangskontrolle:** keine unbefugte Systemnutzung z. B. durch sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern
- **Zugriffskontrolle:** kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems z. B. durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- **Pseudonymisierung:** die Verarbeitung von personenbezogene Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen

Integrität
- **Weitergabekontrolle:** kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B. durch Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
- **Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B. durch Protokollierung, Dokumentenmanagement

Verfügbarkeit und Belastbarkeit
- **Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, zb. B. durch Backup-Strategien (online/offline; onsite/off.site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne
- **Rasche Wiederherstellbarkeit**

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- **Datenschutz-Managemen**t: Nachweis über Beachtung der Grundsätze der Datenverarbeitung
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen**
- **Auftragskontrolle:** keine Auftragsverarbeitung ohne entsprechende Weisung des Auftraggebers, z. B. durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl der Dienstleister, Vorabüberzeugungspflicht, Nachkontrollen

Auch wenn die notwendigen Maßnahmen organisiert sind, ist jede für das Unternehmen tätige Person für die Umsetzung mit verantwortlich. Richtiges Verhalten gemäß Arbeitsvertrag, Verpflichtung auf das Datengeheimnis, IT-Richtlinie und Datenschutzrichtlinie ist unabdingbar.

7. Rechte der Betroffenen
Jede betroffene Person hat die folgenden Rechte
- Recht auf Auskunft über die verarbeiteten personenbezogenen Daten und Zwecke
- Recht auf Berichtigung
- Recht auf Löschung („Recht auf Vergessenwerden")
- Recht auf Einschränkung der Verarbeitung

- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch
- Beschwerderecht bei einer Aufsichtsbehörde
- Widerruf der Einwilligungserklärungen (Widerruf gilt ab Eingang für die Zukunft)

Beim Recht auf Löschung und Recht auf Auskunft gelten die Einschränkungen nach §§ 34 und 35 BDSG

8. Übermittlung in Drittländer (nicht-EU-/EWR-Staaten)
Die Übermittlung in Drittländern (keine Mitgliedsstaaten der Europäischen Union oder Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum) ist nur in sehr beschränkten Ausnahmen zulässig.

9. Haftung
Zuwiderhandlungen gegen die DSGVO bzw. das BDSG sind mit Bußgeld, mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe belegt.
- Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat nach Art. 82 Abs. 1 DSGVO Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
- Jede Aufsichtsbehörde stellt nach Art. 83 Abs. 1 DSGVO sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
- Mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** wird nach § 42 BDSG Abs. 1 bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

- Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird nach § 42 BDSG Abs. 2 bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

- Ordnungswidrig handelt, wer nach § 43 BDSG vorsätzlich oder fahrlässig ein Auskunftsverlagen nicht richtig behandelt oder einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet. Die Ordnungswidrigkeit kann mit einer **Geldbuße** bis zu fünfzigtausend Euro geahndet werden.
- Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird nach § 202a Abs. 1 StGB mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.
- Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmt Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitung verschafft, wird nach § 202b StGB mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
- Wer eine Straftat nach § 202a oder § 202b vorberietet, indem er 1. Passwörter und sonstige Sicherungscodes, die den Zugang zu daten ermöglichen oder 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird nach § 202c Abs. 1 StGB mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.
- Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird nach § 303a Abs. 1 StGB mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft

10. Datenschutzbeauftragter
Bei Fragen zum Datenschutz bzw. zur Datensicherheit oder bei Hinweisen zu Sachverhalten, die Ihrer Meinung nach möglicherweise nicht einer ordnungsgemäßen Datenverarbeitung entsprechen, wenden Sie sich bitte an unseren Beauftragten für den Datenschutz.