

RICHTLINIE ZUM DATENSCHUTZ

Richtlinie zum Datenschutz i.S.d. DSGVO

Version 2.0 / gültig ab 01.05.2021

DE COOR GmbH | Altlaufstraße 38/40 | 85635 Höhenkirchen-Siegertsbrunn | T 08102 8979616 | HRB 194229

AT COOR GmbH | Schillerstraße 27 | 5020 Salzburg | T 0662 452277 | FN 138102t

COOR

Einleitung

Es ist zur alltäglichen Routine geworden IT-Systeme zur Informationsbeschaffung und –verarbeitung sowie zur Kommunikation zu verwenden. Kaum ein Geschäftsbereich kommt heutzutage ohne den Einsatz von Computern aus. Dieser Einsatz erleichtert bei ordnungsgemäßer Benutzung einen Großteil der Tätigkeiten.

Unternehmen haben den Anspruch, möglichst genaue Informationen über ihre Kunden, Lieferanten und Mitarbeiter zu sammeln, um bestmögliche Angebote anbieten zu können. Gerade das Sammeln von Daten muss im Zuge der Datenschutzgrundverordnung (DSGVO) stark eingeschränkt werden, sodass nur die notwendigen Daten (Datenminimierung) eingehoben werden.

Aus diesem Grund sind alle COOR Mitarbeiter zu einem verantwortungsvollen und sorgfältigen Umgang mit unseren Daten und IT-Systemen verpflichtet.

Ziel

Ziel dieser Richtlinie ist es, Mindeststandards für die Nutzung und den Betrieb festzulegen, sowie die rechtskonforme Verarbeitung von personenbezogenen und vertraulichen Daten sicherzustellen.

(1) Erfüllung rechtlicher Anforderungen

Es ist unsere Pflicht den gesetzlichen Anforderungen zu entsprechen, die mit der Erhebung und Verarbeitung personenbezogener Daten verbunden sind.

(2) Erfüllung von Kundenanforderungen

Die Persönlichkeitsrechte und die Privatsphäre eines jeden Einzelnen zu schützen, ist für uns die Basis für eine vertrauensvolle Geschäftsbeziehung.

In unserer Richtlinie zum Datenschutz haben wir strenge Vorgaben für die Verarbeitung personenbezogener Daten von Kunden, Interessenten, Lieferanten, Geschäftspartnern und Mitarbeitern festgelegt. Diese entsprechen den Anforderungen der DSGVO.

Begrifflichkeiten

(1) Verantwortlicher

Ist gem. Art. 4 Abs. 7 DSGVO jene Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter

Ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten

Sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten

Sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrischen Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung

Ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

(6) Aufsichtsbehörde

Ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

(7) ContractCustomer Kunde

Interne COOR Bezeichnung für Kunden, mit denen über die Bestellung hinaus, vertragliche Sondervereinbarungen bestehen.

Anwendungsbereich

Unsere Datenschutzrichtlinie richtet sich nach den Vorgaben der EU-Datenschutzverordnung und den dazugehörigen nationalen Gesetzen. Unsere Datenschutzrichtlinie gilt für die gesamte COOR Gruppe mit all ihren Mitarbeitern an allen Standorten.

Die 7 Grundsätze der Datenverarbeitung

Alle COOR Mitarbeiter sind verpflichtet folgende Grundsätze zur rechtskonformen Speicherung und Verarbeitung personenbezogener Daten einzuhalten.

(1) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise nach Treu und Glauben verarbeitet werden.

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist gegeben, wenn ein Erlaubnistatbestand (Einwilligung, Erfüllung eines Vertrages, Rechtliche Verpflichtung, Berechtigtes Interesse, lebenswichtige Interessen, Öffentliches Interesse) vorliegt.

Die Verarbeitung nach Treu und Glauben bedeutet, dass die betroffene Person mit der Verarbeitung ihrer Daten vernünftigerweise rechnen muss.

Der Grundsatz der Transparenz verlangt, dass die betroffene Person umfassend darüber informiert ist, welche ihrer Daten auf welche Weise verarbeitet und an wen die Daten eventuell übermittelt werden.

Voraussetzung für die Verarbeitung personenbezogener Daten:

- auf rechtmäßige Weise
- nach Treu und Glauben
- in einer für die betroffene Person nachvollziehbaren Weise (Informationspflicht!)

(2) Zweckbindung

Der Grundsatz der Zweckbindung verlangt, dass die Verarbeitung personenbezogener Daten nur für festgelegte, eindeutig und rechtmäßige Zwecke verwendet werden darf. Die Zwecke sind der Person vorab bekanntzugeben. Die Weiterverarbeitung darf den Zwecken der Erhebung nicht widersprechen.

Voraussetzung für die Verarbeitung personenbezogener Daten:

- festgelegte, eindeutige und legitime Zwecke
- darf nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Kopplungsverbot!)

(3) Datenminimierung, Datensparsamkeit, Datennotwendigkeit

Die Datenverarbeitung darf nur soweit erfolgen, als diese für die Erreichung der Zwecke der Verarbeitung unbedingt notwendig ist. Die Menge der Daten und der Umfang der Verarbeitung sind auf das unbedingt erforderliche Ausmaß zu beschränken. Die Daten müssen für die verfolgten Zwecke angemessen und erheblich sein. Ein „Hamstern“ von Daten sollte unterbleiben!

Voraussetzung für die Verarbeitung personenbezogener Daten:

- dem Zweck angemessen und erheblich
- nur dann zulässig, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann
- auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt

(4) Richtigkeit

Personenbezogene Daten müssen ...

- sachlich richtig
- erforderlichenfalls auf dem neuesten Stand sein;
- Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

(5) Speicherbegrenzung, Speicherdauer, Speicherfristen

Der Grundsatz der Speicherbegrenzung verlangt, dass personenbezogene Daten nur so lange gespeichert werden, als diese zur Erreichung der Zwecke der Verarbeitung notwendig ist. Soweit keine gesetzlichen Aufbewahrungsfristen anwendbar sind, muss der Verantwortliche Speicherfristen definieren, die auf das unbedingt notwendige Ausmaß beschränkt sind.

- Ausnahmen: Personenbezogene Daten dürfen länger gespeichert werden,
 - soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden,
 - ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder
 - für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 DSGVO verarbeitet werden.

(6) Integrität und Vertraulichkeit

Bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen ergriffen werden, die die Sicherheit der Daten gewährleisten. Dies umfasst sowohl den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung als auch unbeabsichtigten Verlust/Zerstörung/Schädigung.

- geeignete technische und organisatorische Maßnahmen
- Schutz vor unbefugter oder unrechtmäßiger Verarbeitung
- Schutz vor unbeabsichtigtem Verlust/Zerstörung/Schädigung

(7) Rechenschaftspflicht („Accountability“)

Der Verantwortliche (=COOR) ist für die Einhaltung dieser 7 Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können.

Rechtmäßigkeit der Verarbeitung

Die Verarbeitung personenbezogener Daten ist zulässig, wenn einer der nachstehend angeführten Erlaubnistatbestände vorliegt und es sich nicht um Daten der Kategorie Art. 9 (zB Mitarbeiterdaten) und Art. 10 (zB Strafrelevante Daten) DSGVO handelt.

(1) Einwilligung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene genauestens (ZB über den Zweck, die Datenart und die vermutliche Speicherdauer, ...) informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Die Erteilung der Einwilligung muss dokumentiert werden.

(2) Vertragserfüllung, Vertragsabschluss

Daten von Interessenten, Kunden oder Partners dürfen zur Begründung, Durchführung und Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Kunden oder Partners, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Verträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten, die sie mitgeteilt haben, kontaktiert werden. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten.

(3) Rechtliche Verpflichtung

Die Verarbeitung personenbezogener Daten ist zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten (zB Aufbewahrungspflicht). Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses erforderlich sind.

Für die Entscheidung über die Begründung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsverhältnisses bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

(4) Lebenswichtige Interessen

Die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich. (zB Schutz der körperlichen Gesundheit, notfallmedizinische Behandlung, ...). Dieser Rechtsgrund sollte nur herangezogen werden, wenn kein anderer Rechtsgrund nach Art. 6 DSGVO anwendbar ist.

(5) Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich. Die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person dürfen diesfalls nicht überwiegen.

Beispiele für berechnigte Interessen:

- Betrugsbekämpfung
- Direktwerbung
- Übermittlung von Kunden- u. Mitarbeiterdaten innerhalb einer Unternehmensgruppe
- Sicherstellung der Netz- und Informationssicherheit

Wendet sich der Betroffene mit einem Informationsanliegen an uns (zB Zusendung von Informationsmaterial), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig. Der Betroffene ist vorab über die Verwendung seiner Daten für Zwecke der Werbung zu informieren.

Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene muss über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden. Im Rahmen der Kommunikation soll eine Einwilligung (**Double-Opt-In** zB Anmeldung über Formular + Link zur Bestätigung) des Betroffenen eingeholt werden.

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses erforderlich ist. Berechnigte Interessen sind in der Regel rechtliche (zB Durchsetzung von offenen Forderungen) oder wirtschaftliche (zB Vermeidung von Vertragsstörungen).

Eine Verarbeitung aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn im Einzelfall die Interessen des Betroffenen an dem Schutz seiner Daten gegenüber den berechtigten Interessen an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der COOR Gruppe unterliegt der Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten gemäß Punkt 6.

(1) Empfänger > Subunternehmer

Der Empfänger der Daten (zB Subunternehmer von COOR) muss dazu verpflichtet sein, diese nur zu den festgelegten Zwecken zu verwenden. Zudem muss der Empfänger ein zu diesen Datenschutzrichtlinien gleichwertiges Datenschutzniveau gewährleisten.

Diese Regelungen werden in einer AVV (Vereinbarung zur Auftragsdatenverarbeitung) geregelt. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt.

(2) Empfänger > Kunde

Mit manchen ContractCustomer Kunden hat COOR eine zusätzlich IT-Sicherheitsvereinbarung geschlossen. In dieser kann u.a. geregelt sein, dass

- die Kommunikation nur verschlüsselt stattfinden darf
- nur autorisierte Mitarbeiter des Kunden Weisungen erteilen dürfen
- nur autorisierte Mitarbeiter des Kunden Informationen erhalten dürfen
- nur ausgewählte COOR Mitarbeiter Helpdeskfälle bearbeiten dürfen (Informationen zu Helpdeskfällen erhalten dürfen).

Der Kunde wird als „ContractCustomer“ im Helpdesksystem gekennzeichnet. Bei einer derartigen Kennzeichnung hat sich der COOR Bearbeiter zuvor über die getroffenen und für seine Tätigkeit relevanten IT-Sicherheitsvereinbarungen zu informieren.

AVV = Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist eine Vereinbarung über die Auftragsdatenverarbeitung (=AVV/ADV) zu schließen.

Beispiele:

Auftragnehmer	Verantwortlicher	Daten
COOR	Kunde	COOR Software im SaaS-Betrieb
COOR	Kunde	Datenbearbeitung bei Supportfall
Timr	COOR	Speichern von Mitarbeiterdaten
Microsoft	COOR	Daten in Teams / MS Office 365

Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers (=Verantwortlichen) verarbeiten. Bei der Erteilung des Auftrags sind nachfolgende Vorgaben einzuhalten:

- Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen (TOM) Schutzmaßnahmen auszuwählen.
- Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen und Verantwortlichkeiten des Auftragnehmers und des Verantwortlichen zu dokumentieren.

- Der Verantwortliche ist dazu verpflichtet, sich vor Beginn der Datenverarbeitung zu vergewissern, dass der Auftragnehmer seine Pflichten einhält. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer Zertifizierung nachweisen. Je nach Risiko ist die Kontrolle während der Vertragslaufzeit gegebenenfalls regelmäßig zu wiederholen.

Rechte der Betroffenen

Jeder Betroffene kann die u.a. Rechte wahrnehmen. Ihre Geltendmachung ist umgehend/sofort zu bearbeiten und in jedem Fall ist der Datenschutzbeauftragte zu informieren.

Bei Rechten, die mit **Antrag/Begehren** geltend gemacht werden, muss der Verantwortliche (COOR) innerhalb einer **Frist von einem Monat** auf den Antrag reagieren und entweder

- die gewünschte Maßnahme setzen (also zB die Auskunft erteilen) oder
- begründen, warum er dem Antrag nicht oder nicht vollständig folgt, oder
- mitteilen, dass er auf Grund der Komplexität und der Anzahl von Anträgen noch zwei weitere Monate für eine Antwort benötigt.

(1) Recht auf Geheimhaltung (Art. 1 DSGVO)

Das Recht auf Geheimhaltung personenbezogener Daten ist ein Menschenrecht, welches auf Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) sowie Artikel 7 der Europäischen Grundrechtecharta (Schutz des Privat- und Familienlebens) beruht und in § 1 Datenschutzgesetz ausdrücklich festgehalten ist.

(2) Recht auf Information (Art. 13 und 14 DSGVO)

Werden Daten über Personen erhoben sind diese Personen zum Zeitpunkt der Datenerhebung darüber umfassend in Kenntnis zu setzen.

(3) Recht auf Auskunft (Art. 15 DSGVO)

Jedermann hat das Recht zu erfahren, ob ein Verantwortlicher (Behörde, Unternehmen etc.) Daten zu seiner Person verarbeitet. Um dieses Recht auszuüben, muss der Betroffene ein Begehren an den Verantwortlichen richten. Der Verantwortliche muss die Informationen in einem gängigen elektronischen Format bereitstellen, wenn im Auskunftsbegehren nichts anderes angegeben ist.

(4) Recht auf Berichtigung (Art. 16 DSGVO)

Der Betroffene hat das Recht, von dem Verantwortlichen die Berichtigung ihn betreffender unrichtiger personenbezogener Daten zu verlangen.

(5) Recht auf Löschung (Art. 17 DSGVO)

Der Betroffene hat das Recht auf Löschung seiner Daten in einem der folgenden Fälle:

1. Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
2. Die Verarbeitung beruht auf einer Einwilligung der betroffenen Person, diese widerruft und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
3. Die betroffene Person legt gemäß Artikel 21 Absatz 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt Widerspruch gegen die Verarbeitung für Zwecke der Direktwerbung ein.
4. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

5. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

(6) Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Die Datenschutz-Grundverordnung führt in Art. 18 ein neues Recht auf Einschränkung der Verarbeitung ein. Es dient dazu, den Gebrauch von Daten einzuschränken, ohne sie zu löschen. Die Einschränkung der Verarbeitung kann parallel zum Recht auf Richtigstellung und zum Recht auf Widerspruch verlangt werden.

(7) Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Es gewährt das Recht, Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten einem anderen Verantwortlichen zur Verarbeitung zu geben.

(8) Widerspruchsrecht (Art. 21 DSGVO)

Der Betroffene hat das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung ihn betreffender personenbezogener Daten, die aufgrund von Art. 6 Absatz 1 Buchstaben e oder f DSGVO erfolgt, Widerspruch einzulegen. Die Buchstaben e oder f betreffen die Verarbeitung für eine Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt oder eine Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten. Es gibt weiters ein besonderes Recht auf Widerspruch gegen die Verwendung von Daten für Direktwerbung.

(9) Sonstige Rechte

Gemäß Art. 77 DSGVO hat die betroffene Person das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Datenschutz-Grundverordnung verstößt.

(10) Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen.

Es muss durch geeignete technische und organisatorische Maßnahmen (TOM) eine angemessene Sicherheit gewährleistet werden. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art und Zwecke der Verarbeitung sind geeignete technisch organisatorische Maßnahmen zu treffen, die Folgendes einschließen:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen nach einem Zwischenfall rasch wiederherzustellen.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Sicherheitsmaßnahmen (Datenschutzmanagement; Art. 32 Abs. 1 Buchst. d) DSGVO), sowie ein Sicherheitskonzept, das die getroffenen Maßnahmen darstellt (vgl. Art 5 Abs. 2 DSGVO) sind in Umsetzung.

Verpflichtung zur Einhaltung der Richtlinie

Diese Richtlinie wurde mir erläutert, ich habe sie in Kopie erhalten und ich verpflichte mich diese Richtlinie vollumfänglich einzuhalten.

Richtlinie: Richtlinie zum Datenschutz

Version: 2.0

Datum: Gültig ab 01.05.2021

Vor-/Nachname: _____

Abteilung: _____

Datum: _____

Unterschrift: _____

Bitte ausdrucken, unterfertigen und an datenschutz@coor.info mailen.