Datenschutz-Richtlinie

Die VIVAVIS AG - nachfolgend „VIVAVIS“ genannt - bündelt die unternehmerischen Aktivitäten einer mittelständischen Unternehmensgruppe. Zu VIVAVIS gehören alle Tochtergesellschaften der VIVAVIS AG sowie deren Beteiligungen.

1 Ziel der Datenschutzrichtlinie

Daten und Informationen sind wesentliche Faktor von Geschäftsprozessen sowie zu deren Automatisierung und Optimierung notwendig. Die Digitalisierung und Vernetzung verbessert die Möglichkeiten und Nutzung von Daten zusätzlich. Die Verarbeitung personenbezogener Daten ist nur in den gesetzlich geregelten Fällen zulässig. Zudem muss ein hohes Maß an Datenschutz gewährleistet sein. Dies gilt für Daten von natürlichen Personen (personenbezogene Daten), d.h. Daten mit direktem Personenbezug oder Daten von denen auf ein Individuum geschlossen werden kann.

Die Wahrung der Persönlichkeitsrechte (insbesondere das Recht auf informationelle Selbstbestimmung) und der Privatsphäre eines jeden Einzelnen ist nicht nur ein hohes rechtliches Gut, sondern wird von uns auch als Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der VIVAVIS als attraktiver Arbeitgeber verstanden. Daher räumen wir der Erfüllung der gesetzlichen Anforderungen des Datenschutzes die notwendige Priorität ein.

VIVAVIS verpflichtet sich im Rahmen ihrer gesellschaftlichen und sozialen Verantwortung zur Einhaltung der Vorgaben aus der Datenschutzgrundverordnung (DSGVO). In einigen Ländern und Regionen, wie der Europäischen Union, hat der Gesetzgeber Standards für den Schutz der Daten von natürlichen Personen („personenbezogene Daten“) festgelegt, einschließlich der Anforderung, dass diese Daten nur dann in andere Länder übermittelt werden dürfen, wenn am Bestimmungsort ein angemessenes Datenschutzniveau beim Empfänger besteht.

Die Datenschutzrichtlinie der VIVAVIS legt einheitliche und angemessene, unternehmensinterne Datenschutzstandards fest – sowohl für:

(a) die Verarbeitung personenbezogener Daten in Regionen wie der EU / dem Europäischen Wirtschaftsraum (EWR) (nachstehend einheitlich als „EU“ bezeichnet) als auch

(b) die grenzüberschreitende Übermittlung personenbezogener Daten an Unternehmen außerhalb der EU.

Zu diesem Zweck gibt diese Richtlinie verbindliche Regeln für die Verarbeitung personenbezogener Daten mit EU-Herkunft innerhalb der VIVAVIS vor.

2 Geltungsbereich und Aktualisierung der Datenschutzrichtlinie

Diese Datenschutzrichtlinie gilt für alle Unternehmen der VIVAVIS und alle von ihr abhängigen Konzerngesellschaften sowie verbundenen Unternehmen sowie deren Führungskräfte und Mitarbeiter. Damit gilt diese Richtlinie für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten.

Die einzelnen Konzerngesellschaften sind nicht berechtigt, von dieser Datenschutzrichtlinie abweichende Regelungen zu treffen. Weitere Richtlinien zum Datenschutz dürfen in Abstimmung mit dem Datenschutzbeauftragten dann erstellt werden, wenn dies nach dem jeweiligen nationalen Recht erforderlich ist. Sollte eine Abweichung von den Vorgaben dieser Richtlinie zwingend notwendig werden, ist vorher die Freigabe der Compliance-Abteilung – Datenschutzbeauftragte einzuholen.

Eine Aktualisierung dieser Datenschutzrichtlinie findet in Abstimmung mit dem Datenschutzbeauftragten innerhalb des für die Änderung von Richtlinien vorgegebenen Verfahrens statt. Die Änderungen werden den Unternehmen der VIVAVIS unverzüglich gemeldet.

Die aktuellste Version der Datenschutzrichtlinie kann unter den Datenschutzhinweisen auf der Internetseite der VIVAVIS, **www.vivavis.com**, abgerufen werden.

3 Umsetzung staatlichen Rechts

Diese Datenschutzrichtlinie ersetzt nicht die EU-Vorschriften und die nationalen Gesetze. Sie ergänzt die nationalen und internationalen Datenschutzgesetze. Diese Vorschriften und Gesetze haben Vorrang, wenn die Einhaltung dieser Richtlinie zu einem Verstoß gegen geltendes Recht führen würde. Der Inhalt dieser Richtlinie ist jedenfalls auch dann zu beachten, wenn es keine entsprechenden (nationalen) Gesetze gibt.

Jedes Unternehmen der VIVAVIS ist für die Einhaltung dieser Datenschutzrichtlinie und der gesetzlichen Verpflichtungen verantwortlich. Sollte die Einhaltung dieser Richtlinie gegen nationales Recht verstoßen, ist im Konfliktfall zwischen nationaler Gesetzgebung und dieser Richtlinie eine praktikable Lösung zu erarbeiten und in die Richtlinie einzubinden. Hat es Grund zu der Annahme, dass gesetzliche Verpflichtungen im Widerspruch zu den Pflichten aus dieser Datenschutzrichtlinie stehen, hat das betroffene Konzernunternehmen unverzüglich den Datenschutzbeauftragten zu informieren.

4 Prinzipien für die Verarbeitung personenbezogener Daten

4.1 Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden.

4.2 Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Sofern die erhobenen Daten zu einem anderen, als dem ursprünglich festgelegten Zweck verarbeitet werden sollen muss der „neue“ Zweck hinreichend und konkret festgelegt werden. Darüber hinaus muss die betroffene Person vor der Weiterverarbeitung zu einem anderen Zweck Informiert werden, ggf. ist eine erneute Zustimmung der betroffenen Personen notwendig.

4.3 Transparenz

4.4 Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- die Identität der verantwortlichen Stelle
- den Zweck der Datenverarbeitung
- Dritte, an die die Daten gegebenenfalls übermittelt werden

4.5 Datenminimierung

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch nationale Recht vorgeschrieben oder erlaubt.

4.6 Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind (Erreichen der Zweckbindung), müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde.

4.7 Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten müssen sachlich richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand sein. Es sind durch die Verantwortlichen angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt oder aktualisiert werden.

4.8 Integrität und Vertraulichkeit

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen 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").

5 Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

5.1 Kunden- und Partnerdaten

5.1.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, Durchführung und Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Kundenbetreuung, 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 Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden. Vom Interessenten geäußerte Einschränkungen sind zu beachten.

5.1.2 Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an ein Unternehmen der VIVAVIS (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

Kundenbindungs- oder Werbemaßnahmen bedürfen weiterer rechtlicher Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist 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 mit dem Betroffenen, muss eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden. Der Betroffene soll im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, E-Mail und Telefon wählen können. Eine solchermaßen gegebene Einwilligung muss jederzeit widerrufen werden können.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden. Darüber hinaus bestehende Beschränkungen einiger Länder bezüglich der Verwendung von Daten für Werbezwecke sind zu beachten.

5.1.3 Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene über die Verarbeitung und auch über die entsprechende Widerrufsmöglichkeit mit Wirkung für die Zukunft informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.

5.1.4 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten (vgl. Artikel 6, Abs. 1 lit. c und d DSGVO). Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

5.1.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der VIVAVIS erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen oder Grundrechte des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen, eine solche Prüfung ist ggf. zu dokumentieren.

5.1.6 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger, personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

5.1.7 Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden und zu negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen führen können, sind untersagt.

5.1.8 Nutzerdaten und Internet

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden.

Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

5.2 Mitarbeiterdaten

5.2.1 Datenverarbeitung für Arbeitsverhältnisse

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung 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 Arbeitsvertrages bezogen sein, sofern nicht einer der folgenden Erlaubnistatbestände für die Datenverarbeitung greift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

5.2.2 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

5.2.3 Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall dokumentiert werden. Der Betroffene muss über die Verarbeitung und auch über die entsprechende Widerrufsmöglichkeit mit Wirkung für die Zukunft informiert werden.

5.2.4 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der VIVAVIS erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z.B. Bewertung von Unternehmen) begründet.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Informationsrechte der Betroffenen) berücksichtigt werden.

5.2.5 Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

5.2.6 Automatisierte Entscheidungen

Automatisierte Verarbeitungen besonders schutzwürdige personenbezogene Daten, durch die einzelne Persönlichkeitsmerkmale bewertet werden und zu negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen führen können, sind untersagt.

5.2.7 Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet werden vornehmlich im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden. Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das jeweils nationale geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in die Netze der VIVAVIS implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der VIVAVIS erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Regelungen der VIVAVIS zur Informationssicherheit.

6 Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der VIVAVIS oder an Empfänger innerhalb der VIVAVIS unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt 5. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

Im Falle einer Datenübermittlung an einen Empfänger außerhalb der VIVAVIS in einem Drittstaat muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Eine solche gesetzliche Verpflichtung kann sich aus dem Recht des Sitzlandes der Konzerngesellschaft, welche die Daten übermittelt, ergeben oder das Recht des Sitzlandes der Konzerngesellschaft erkennt das mit der gesetzlichen Verpflichtung eines Drittstaats verfolgte Ziel der Datenübermittlung an.

Im Falle einer Datenübermittlung von Dritten an Unternehmen der VIVAVIS muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

Die Übermittlung personenbezogener Daten von einer Konzerngesellschaft mit Sitz im Europäischen Wirtschaftsraum an einen Empfänger mit Sitz außerhalb des Europäischen Wirtschaftsraums (Drittstaat) bedarf der Zustimmung durch die Geschäftsführung der VIVAVIS und erfolgt nur auf Basis des Art. 44ff DSGVO (Datenübermittlung in ein Drittland).

Soweit personenbezogene Daten an Dritte übermittelt werden, z.B. im Rahmen der Teilnahme an Ausschreibungen oder sonstiger Bewerbungen der VIVAVIS AG um Aufträge, gilt grundsätzlich folgendes:

- Es werden im Rahmen der Datenminimierung nur diejenigen Daten übermittelt, an denen die Gegenseite, z.B. ein Auftraggeber, ein berechtigtes Interesse hat. VIVAVIS wird geeignete Maßnahmen ergreifen, um sicherzustellen, dass nur das notwendige Minimum an Daten übermittelt wird, z.B. besondere Lebensläufe von Mitarbeitern, die nur das notwendige Minimum an Daten enthalten, verwenden.
- Soweit eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der EU oder einem anderen Drittstaat mit vergleichbarem Schutzniveau erfolgen soll, wird vorher die ausdrückliche Einwilligung des betroffenen Mitarbeiters eingeholt. Eine solche Einwilligung kann vorab erteilt werden, sie ist jedoch spätestens alle 3 Jahre zu erneuern und kann jederzeit widerrufen werden. Die Einwilligung ist in jedem Fall zu dokumentieren.

7 Auftragsverarbeitung

Eine Auftragsverarbeitung 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 sowohl mit externen Auftragnehmern als auch zwischen Unternehmen innerhalb der VIVAVIS eine Vereinbarung über eine Auftragsverarbeitung abzuschließen. Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss ihre Umsetzung sicherstellen:

(1) Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.

(2) Der Auftrag ist mindestens in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.

(3) Die Verträge sollten den Anforderungen der DSGVO entsprechen.

(4) Der Auftraggeber muss vor Beginn der Datenverarbeitung einen Auftragsverarbeitungsvertrag abschließen und sich von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Regelmäßige Kontrollen sind durch den Auftraggeber oder von ihm beauftragte Dritte durchzuführen.

(5) Bei einer grenzüberschreitenden Auftragsverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftraggeber die Standarddatenschutzklauseln (SCC´s) und ggf. zusätzliche Maßnahmen vereinbart hat.

8 Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist im Rahmen der gesetzlichen Fristen umfangreich durch eine zentrale Stelle zu bearbeiten und darf für den Betroffenen zu keinen Nachteilen führen.

(1) Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers Auskunft gegeben werden.

(2) Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

(3) Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.

(4) Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

(5) Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

Darüber hinaus kann jeder Betroffene die oben genannten, eingeräumten Rechte als Drittbegünstigter geltend machen, wenn ein Unternehmen, das sich zur Einhaltung der Datenschutzrichtlinie verpflichtet hat, deren Vorgaben nicht beachtet und er dadurch in seinen Rechten verletzt ist.

9 Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-Know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Vorgesetze müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

10 Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren. Der verantwortliche Fachbereich kann dazu insbesondere seinen Informationssicherheitsbeauftragten (ISB) und Datenschutzbeauftragten (DSB) zu Rate ziehen.

Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des konzernweiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

11 Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem Datenschutzbeauftragten oder beauftragten externen Prüfern. Der Vorstand der VIVAVIS AG ist im Rahmen der jeweiligen Berichtspflichten über wesentliche Ergebnisse zu informieren.

Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutz-aufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

12 Verantwortlichkeiten und Sanktionen

Die Vorstände und Geschäftsführungen der Konzerngesellschaften sind verantwortlich für die Datenverarbeitung in ihrem Verantwortungsbereich. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. nationale Meldepflichten). Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehend zu informieren.

Die jeweiligen Vorstände und Geschäftsführungen müssen dem Datenschutzbeauftragten einen Datenschutzkoordinator benennen. Die Datenschutzkoordinatoren sind vor Ort Ansprechpartner für den Datenschutz. Diese können Kontrollen durchführen und haben die Mitarbeiter mit den Inhalten der Datenschutzrichtlinien vertraut zu machen. Die jeweiligen Vorstände und Geschäftsführungen sind verpflichtet, den Datenschutzbeauftragten und die Datenschutzkoordinatoren in ihrer Tätigkeit zu unterstützen.

Die für Geschäftsprozesse fachlich Verantwortlichen müssen den Datenschutzbeauftragten rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der

Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten.

Die Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter regelmäßig und im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

13 Datenschutzbeauftragter und Datenschutzkoordinatoren

Der Datenschutzbeauftragte für den Datenschutz als fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er unterstützt und überwacht die Einhaltung der Richtlinien zum Datenschutz. Der Datenschutzbeauftragte wird vom Vorstand der VIVAVIS AG bestellt.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten oder den Datenschutzkoordinator des jeweiligen Standortes wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Kann der zuständige Datenschutzkoordinator einer Beschwerde nicht abhelfen oder einen Verstoß gegen Datenschutzrichtlinien nicht abstellen, muss er den Datenschutzbeauftragten der VIVAVIS einschalten. Die Entscheidungen des Datenschutzbeauftragten zur Abhilfe der Datenschutzverletzung sind durch die jeweiligen Vorstände und Geschäftsführungen zu berücksichtigen. Anfragen von Aufsichtsbehörden sind immer mit dem Datenschutzbeauftragten abzustimmen.

Der Datenschutzbeauftragte kann wie folgt erreicht werden:
Kamm, Susanne – Email: datenschutz@dornbach-consulting.de – Phone: +49 261 9431 441

Datenschutzkoordinatoren an den Standorten sind:

Bochum:
Volker Lange – Email: volker.lange@vivavis.com – Phone: +49 234 9325 133

Ettlingen/Berlin/Dreieich:
Dr. Ralf Thomas – Email: ralf.thomas@vivavis.com – Phone: +49 7243 218 743

Koblenz:
Christoph Becher – Email: christoph.becher@vivavis.com – Phone: +49 261 9285 332

Für das übergeordnete Compliance-Management zeichnet verantwortlich:

Chief Compliance Officer:
RA Volker Motzkus – Email: volker.motzkus@vivavis.com – Phone: +49 7243 218 851

14 Glossar

Ein **angemessenes Datenschutzniveau von Drittstaaten** wird von der EU Kommission dann anerkannt, wenn der Kernbestand der Privatsphäre, so wie er in den Mitgliedstaaten der EU übereinstimmend verstanden wird, im Wesentlichen geschützt wird. Die EU Kommission berücksichtigt bei ihrer Entscheidung alle Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Dies schließt die Beurteilung staatlichen Rechts sowie der jeweiligen geltenden Standesregeln und Sicherheitsmaßnahmen ein.

Anonymisiert sind Daten dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.

Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

Betroffener im Sinne dieser Datenschutzrichtlinie ist jede natürliche Person, über die Daten verarbeitet werden. In einigen Ländern können auch juristische Personen Betroffener sein.

Datenschutzvorfälle sind alle Ereignisse, bei denen der begründete Verdacht besteht, dass personenbezogene Daten rechtswidrig ausgespäht, erhoben, verändert, kopiert, übermittelt oder genutzt wurden. Das kann sich sowohl auf Handlungen durch Dritte als auch Mitarbeiter beziehen.

Dritter ist jeder außerhalb des Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle. Auftragsverarbeiter sind innerhalb der EU nicht Dritte im Sinne des Datenschutzrechtes, da sie gesetzlich der verantwortlichen Stelle zugeordnet sind.

Drittstaaten im Sinne der Datenschutzrichtlinie sind alle Staaten außerhalb der Europäischen Union/EWR. Ausgenommen sind Staaten, deren Datenschutzniveau von der EU Kommission als angemessen anerkannt worden ist.

Einwilligung ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.

Erforderlich ist die Verarbeitung personenbezogener Daten, wenn der zulässige Zweck oder das berechtigte Interesse ohne die jeweiligen personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand zu erreichen ist.

Der **Europäische Wirtschaftsraum (EWR)** ist ein mit der EU assoziierter Wirtschaftsraum, dem Norwegen, Island und Liechtenstein angehören.

Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z.B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann.

Übermittlung ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.

Verarbeitung personenbezogener Daten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang zur Erhebung, Speicherung, Organisation, Aufbewahrung, Veränderung, Abfrage, Nutzung, Weitergabe, Übermittlung, Verbreitung oder der Kombination und der Abgleich von Daten. Dazu gehört auch das Entsorgen, Löschen und Sperren von Daten und Datenträgern.

Verantwortliche Stelle ist diejenige juristisch selbständige Gesellschaft der Unternehmensgruppe VIVAVIS, deren Geschäftsaktivität die jeweilige Verarbeitungsmaßnahme veranlasst.

15 Mitgeltende Unterlagen

CoC Code of Conduct der VIVAVIS

16 Dokument-Information / Änderungsangaben

Ablage:	VIVAVIS AG	**zust. Stelle:**		Vorstand
Dok. Nr.:	Datenschutzrichtlinie	erstellt -> geprüft -> freigegeben		
Dokument-Ausgabe / Beschreibung der Änderung		**Datum**	**Abt**	**Name**
01	Erstausgabe	16.04.2018	IDS-H	R. Thomas
		16.04.2018	IDS-H	J. Schaden
		08.05.2018	IDS-H	N. Wagner
02	Umfirmierung in VIVAVIS GmbH	31.08.2019	VIVAVIS	R. Thomas
		31.08.2019	VIVAVIS	R. Thomas
		31.08.2019	VIVAVIS	N. Wagner
03	Umfirmierung auf VIVAVIS AG - Anpassung auf neue Unternehmensstruktur - Aktualisierung der Ansprechpartner	18.12.2020	Z-DS	R. Thomas
		30.03.2021	DSB	S. Kamm
		06.05.2021	Vorstand	C. v. Dinther