Datenschutz- und Datensicherheitsleitlinie der

Neo Consult GmbH & Co. KG

Verantwortliche Stelle

Neo Consult GmbH & Co. KG

Haspelstraße 35
35037 Marburg
Tel: 06421 4994490
Fax: 06421 4994491
Email: info@neoconsult.de
www.neoconsult.de

Inhalt

I. Sinn und Zweck dieser Datenschutzrichtlinie

Die Neo Consult GmbH & Co. KG (nachfolgend „Verantwortliche Stelle") verpflichtet sich im Rahmen ihres Auftretens am Markt zur Einhaltung der Datenschutzrechte. Diese Datenschutzrichtlinie gilt für sämtliche Bereiche der Verantwortlichen Stelle und fußt auf den europäischen und nationalen Grundprinzipien zum Datenschutz.

Die Einhaltung des Datenschutzes ist für uns Pflicht und Kür für eine vertrauensvolle Geschäftsbeziehung zu unseren Kunden. So ist gewährleistet, dass das von der Europäischen Datenschutzrichtlinie (DS-GVO) und den nationalen Gesetzen (bspw. BDSG n.F.) ausgehende und verlangte Schutzniveau gewahrt bleibt.

II. Geltungsbereich und Änderung dieser Datenschutzrichtlinie

Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten[1]. Anders als nicht-anonymisierte Daten unterliegen die anonymisierten Daten bspw. für statistische Auswertungen oder Untersuchungen, nicht dieser Datenschutzrichtlinie.

Eine Änderung dieser Datenschutzrichtlinie erfolgt nur in enger Abstimmung mit dem Datenschutzbeauftragten bzw. der Geschäftsleitung.

Die jeweils neueste Version der Datenschutzrichtlinie kann auf der Internetseite der Verantwortlichen Stelle unter
https://neoconsult.de/datenschutz.php
und unter
https://neo-consult.de/datenschutz/
eingesehen werden.

III. Geltung nationalen Rechts

Die vorliegende Datenschutzrichtlinie ist ergänzend zum geltenden nationalen Datenschutzrecht zu lesen und deckt auch die Datenschutzprinzipien der Europäischen Union umfassend ab. Dabei geht das nationale Recht (bspw. BDSG n.F.), nur dann der Datenschutzgrundverordnung mit ihrer unmittelbaren Wirkung vor, wenn ein Aspekt durch die Verordnung nur rudimentär umschrieben und der Konkretisierung bedarf. Hat entgegen aller Erwartung der nationale Gesetzgeber keine dieser Datenschutzrichtlinie entsprechende Regelung vorgesehen, so setzt diese Datenschutzrichtlinie gleichwohl verbindliches Recht für den Verantwortlichen.

Im Übrigen werden die Meldepflichten für eine etwaige Datenverarbeitung stets beachtet.

[1] **Vgl. XV**

Im Falle eines Widerspruches zwischen den gesetzlichen Regelungen der Bundesrepublik Deutschland zum Datenschutz und dieser Datenschutzrichtlinie, wird der Verantwortliche nach einer gesetzeskonformen Lösung im Sinne dieser Datenschutzrichtlinie suchen.

IV. Grundsätze für die Verarbeitung personenbezogener Daten

1. Rechtmäßigkeit

Im Rahmen der Verarbeitung personenbezogener Daten sind die Persönlichkeitsrechte des Betroffenen[2] zu wahren. Deshalb müssen personenbezogene Daten bereits gesetzes- und regelkonform erhoben und verarbeitet werden.

2. Zweckbindung

Der jeweilige Zweck für den die personenbezogenen Daten erhoben und verarbeitet worden sind, ist bereits zuvor zu definieren. Eine etwaige nachträgliche Änderung dieses vorher festgelegten Erhebungszwecks ist nur bedingt möglich und bedarf zu seiner Wirksamkeit einer überzeugenden Rechtfertigung.

3. Transparenz

Der Betroffene muss über die Verwendung seiner Daten in Kenntnis gesetzt werden. Auch sind die personenbezogenen Daten bei dem Betroffenen selbst zu erheben. Bei der Erhebung ist der Betroffene über nachfolgende Punkte in Kenntnis gesetzt worden bzw. waren diese Punkte für ihn ersichtlich:

- **den Zweck der Datenverarbeitung**
- **die Verantwortliche Stelle**
- **Dritte an die die Daten des Betroffenen weitergegeben werden könnten (sog. Übermittlung). Hierbei ist allerdings zu berücksichtigen, dass die Verantwortliche Stelle auch Gruppen von Empfängern definieren kann, wenn es der Übersichtlichkeit und Transparenz der Informationsverpflichtung dient.**

4. Sparsamkeit und Vermeidung von Daten

Bereits vor der Verarbeitung personenbezogener Daten ist die Notwendigkeit der Erhebung bzw. der Erhebungsumfang zur Zweckerreichung zu prüfen. Immer dort, wo es zur Zweckerreichung ausreichend und der betriebliche Aufwand in einem angemessen Verhältnis stehend ist, sind anonymisierte bzw. statistische Daten zu nutzen.

So dürfen personenbezogene Daten auch nicht auf Vorrat für mögliche zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch das nationale Recht vorgeschrieben oder sogar ausdrücklich erlaubt.

5. Löschung

Nach dem Ablauf der geschäftsbedingten bzw. gesetzlichen Aufbewahrungsfristen, müssen personenbezogene Daten, die nicht mehr erforderlich[3] sind, gelöscht werden.

[2] **vgl. Definition unter XV**

Abweichend davon, müssen Daten, die ein schutzwürdiges Interesse (bspw. nach HGB) oder historische Bedeutung (Unternehmensarchiv) genießen, weiterhin gespeichert bleiben, bis das schutzwürdige Interesse bzw. die historische Bedeutung rechtlich abschließend geklärt worden ist.

6. Aktualität und sachliche Richtigkeit der Daten

Die erhobenen personenbezogenen Daten sind korrekt, vollständig und wenn erforderlich auch auf dem neuesten Stand zu speichern. Dementsprechend sind angemessene Regelungen zu treffen, die gewährleisten, dass nicht zutreffende, unvollständige oder überholte Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

7. Sicherheit und Vertraulichkeit der Daten

Das Datengeheimnis gilt für personenbezogene Daten. Diese müssen in der persönlichen Interaktion vertraulich behandelt werden. Um die widerrechtliche Verarbeitung oder Weitergabe zu verhindern bzw. dem Verlust, der Veränderung oder der Zerstörung entgegenzuwirken, müssen angemessene, organisatorische und auch technische Maßnahmen eingesetzt werden, die einen unberechtigten Zugriff auf diese Daten Einhalt gebieten.

V. Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit einer der abschließend aufgezählten Erlaubnistatbestände gegeben ist. Diese Erlaubnis ist auch erforderlich bzw. gilt auch in Fällen, in denen der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten geändert werden soll.

1. Kunden- und Partnerdaten

1.1 Datenverarbeitung im Rahmen vertraglicher Beziehungen

Die personenbezogenen Daten der Kunden dürfen zur Begründung, Durchführung und Beendigung eines Vertrages (bspw. Versicherungsvertrages, Maklervertrages, Kooperationsvertrages, Vergleichsportalnutzungsvertrages, etc.) verarbeitet werden. Davon betroffen ist auch die Betreuung (z.B. Bestandspflege, Bestandsübertragungen, etc.), soweit diese in Konnexität zum Vertragszweck steht.

Auch in der vorvertraglichen Phase (also während der Anbahnung des Vertrages) ist es erlaubt, personenbezogene Daten zur Erstellung von Angeboten des potentiellen Vertragspartners zu verarbeiten. Insbesondere um die Wünsche des potentiellen Vertragspartners im Hinblick auf den Vertragsabschluss ausreichend berücksichtigen zu können. Deshalb ist es auch erlaubt, während der Anbahnungsphase mit Hilfe (Nutzung) der bis hierhin durch den potentiellen Vertragspartner mitgeteilten Daten, Kontakt zu eben diesem aufzunehmen. Die vom Verantwortlichen erhobenen Daten des Kunden werden dabei zunächst an eine Abwicklungsstelle versandt, welche dann wiederum im Rahmen der Abwicklung an den jeweiligen Produktpartner weitergeleitet werden.

[3] **vgl. Definition unter XV**

Zu beachten sind dabei jedoch etwaig mit der Datenmitteilung kundgetane Einschränkungen des potentiellen Vertragspartners. Die davon zu trennenden Werbemaßnahmen sind unter V. 1.2 gesondert geregelt und unterliegen besonderen Voraussetzungen.

1.2 Verarbeitung zwecks Werbung

Die Datenverarbeitung zum Zwecke der Erfüllung eines Anliegens eines Betroffenen ist zulässig. Etwa, wenn sich ein Betroffener zum Zwecke der Information an den Verantwortlichen wendet (bspw. Newsletter, Imagebrochüren oder sonstigen Informationsmaterial zu Versicherungsprodukten etc.).

Werbemaßnahmen die der Kundenbindung dienen, unterliegen weiteren rechtlichen Voraussetzungen. Die Verarbeitung personenbezogener Daten zwecks Werbung ist nur zulässig, wenn der ursprüngliche Erhebungszweck der Daten diese Verwendung noch abdeckt. Die Verwendung der Daten zur Werbung ist dem Betroffenen mitzuteilen.

Daten die ausschließlich zu Werbezwecken erhoben werden, sind für den Betroffenen nicht verpflichtend mitzuteilen. Über diese Freiwilligkeit ist der Betroffene auch zu informieren. Im Rahmen der Interaktion mit dem Betroffenen ist eine Einwilligung[4] in die Verarbeitung seiner Daten zu Werbezwecken einzuholen. Dabei soll der Betroffene zwischen den innerhalb der Verantwortlichen Stelle angewandten Kontaktkanälen (Post, elektronische Post, Fax, Telefon) wählen können.

Hat der Betroffene der Verwendung seiner Daten zu Werbezwecken explizit widersprochen, so ist eine Verwendung für diese Zwecke unzulässig. Die Daten sind dann bereits ab Erhebung für diese Form der Verwendung zu sperren. (sog. Werbesperre).

1.3 Einwilligung in die Verarbeitung

Die Datenverarbeitung ist neben den Anlässen der Ziff. V. 1.1 stets möglich, wenn eine ausdrückliche Einwilligung des Betroffenen in diese vorliegt. Der Betroffene ist bereits vor der Einwilligung im Umfang des IV. 3.[5] zu informieren. Dem Betroffenen ist die Einwilligungserklärung aus Darlegungs- und Beweisgründen stets schriftlich oder auf elektronischem Wege abzufordern. In bestimmten Bereichen (z.B. der Investmentberatung) ist die Erteilung der Einwilligung auf mündlichem Wege möglich, unterliegt dann jedoch der Dokumentationspflicht.

1.4 Verarbeitung aufgrund gesetzlicher Erlaubnis

Dem Gedanken des Grundsatzes vom Vorbehalt des Gesetzes folgend, ist eine Verarbeitung personenbezogener Daten zudem immer zulässig, wenn eine gesetzliche Regelung die Datenverarbeitung verlangt, auf dieser aufbaut oder eine solche schlicht gestattet.

[4] Vgl. dazu V. 1.3
[5] Vgl. dazu IV. 3.

Dabei richten sich Art und Umfang der Datenverarbeitung nach den gesetzlichen Regelungen und müssen auch erforderlich[6] sein.

1.5 Verarbeitung wegen eines berechtigten Interesses

Personenbezogene Daten können auch dann verarbeitet werden, wenn dies zur Verwirklichung eines berechtigten Interesses des Verantwortlichen erforderlich ist. Zu diesen berechtigten Interessen zählen vor allem solche, rechtlicher (bspw. Forderungsdurchsetzung) und wirtschaftlicher (bspw. um die Vertragsdurchführung zu gewährleisten) Art. Einer Verarbeitung kann im Einzelfall das, im Rahmen einer Abwägung höher gewichtete, schutzwürdige Interesse des Betroffenen entgegenstehen. Vor jeder Verarbeitung ist deshalb eine Prüfung dahingehend vorzunehmen, ob schutzwürdige Interessen des jeweils Betroffenen bestehen und wenn ja wie diese zu gewichten sind.

1.6 Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen verarbeitet werden, soweit der Betroffene ausdrücklich seine darauf bezogene Einwilligung erklärt hat oder das Gesetz die Verarbeitung als erforderlich festschreibt. Eine zwingende Notwendigkeit der Datenverarbeitung begründet deren Zulässigkeit und ist gegeben, wenn dadurch rechtliche Ansprüche gegenüber dem Betroffenen geltend gemacht, ausgeübt oder verteidigt werden können.

Zeichnet sich die alsbaldige Datenverarbeitung besonders schutzwürdiger Interessen ab, so ist der Datenschutzbeauftragte des Verantwortlichen vor der tatsächlichen Verarbeitung zu informieren.

1.7 Automatisierte Entscheidung im Einzelfall

Der Fortschritt ermöglicht technisch sogenannte automatisierte Einzelentscheidungen. Gleichwohl dürfen diese nicht die ausschließliche Grundlage für Entscheidungen mit abschlägigen rechtlichen Folgen oder gar erheblichen Beeinträchtigungen für den Betroffenen sein. Das diesem automatisierten Entscheidungsprozess entspringende Ergebnis ist neben der Information über den Einsatz der automatisierten Form, dem Betroffenen zusammen mit einer Möglichkeit zur Stellungnahme mitzuteilen. Das Risiko einer automatisierten Fehlentscheidung muss durch eine Plausibilitätsprüfung eines Mitarbeiters minimiert bzw. annähernd ausgeschlossen werden.

1.8 Internetauftritt und Nutzerdaten

Die Betroffenen sind über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf den Webseiten und Apps des Verantwortlichen in den Datenschutz- und Cookie-Hinweisen zu informieren. Dabei sind die Datenschutz- und Cookie-Hinweise leicht erkennbar, unmittelbar erreichbar und dauerhaft verfügbar für den Betroffenen zu implementieren.

Der Verantwortliche informiert den potentiell Betroffenen in den Datenschutzhinweisen auch über eine etwaige Auswertung oder Anfertigung eines Nutzungsprofils[7] über

[6] **Vgl. XV.**

das Nutzungsverhalten von Webseiten- und App-Benutzern (bspw. Klickzahlen bei Newslettern, frei zugänglichen Webinaren oder Downloadzahlen der online bereitgestellten Muster-Maklerverträge).

Ein solches Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder aber der Betroffene seine Einwilligung gegeben hat.

Wird das Tracking unter Verwendung eines Pseudonyms durchgeführt, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden.[8]

2. Mitarbeiterdaten

2.1 Datenverarbeitung das (sich anbahnende) Arbeitsverhältnis betreffend

Die Begründung, die Durchführung oder die Beendigung des Arbeits-, Anstellungs- oder Dienstverhältnisses kann eine Verarbeitung personenbezogener Daten erforderlich machen. Ist dies der Fall, so darf sie erfolgen. Insbesondere bei der Anbahnung eines Arbeitsverhältnisses ist eine Verarbeitung von erhaltenen personenbezogenen (Bewerber-)Daten erlaubt. Die erhaltenen (Bewerber-)Daten sind unter Berücksichtigung beweisrechtlicher Fristen nach einer erteilten Ablehnung zu löschen. Dies gilt nicht, wenn der Bewerber in eine erneute Verwendung seiner Daten zu einem späteren Zeitpunkt im Rahmen eines erneuten Auswahlverfahrens gegebenenfalls auch innerhalb der Verantwortlichen Stelle eingewilligt hat.

Ist der Auswahlprozess ausgegliedert und wird mit Hilfe externer Dritte durchgeführt, so stellt die Verantwortliche Stelle vertraglich sicher, dass mit Mitarbeiterdaten *DS-GVO compliant* umgegangen wird.

Eine Einwilligung hat stets auch dann zu erfolgen, wenn die (Bewerber-)Daten aus dem ursprünglichen Bewerbungsprozess in einem späteren erneuten Auswahlverfahren bezüglich gleicher oder eine andere Position betreffend gewünscht ist.

Die Verarbeitung der (Bewerber-)Daten hat sich stets am Zweck des Arbeitsvertrages zu orientieren und darf nur in den nachfolgend abschließend aufgezählten Ausnahmefällen davon abweichen:

Bei einer erforderlichen Erhebung weiterer Informationen über den Bewerber bei Dritten, während der Anbahnungsphase des Arbeitsverhältnisses, hat sich diese an den gesetzlichen Regelungen der Bundesrepublik Deutschland zu orientieren. Bei verbleibenden Zweifeln der Verantwortlichen Stelle ist zur Wahrung der Rechtmäßigkeit der Erhebung eine Einwilligung bezogen auf die weiteren Informationen nötig.

Werden personenbezogene Daten nicht explizit für die Durchführung des Arbeitsverhältnisses verarbeitet, ist jeweils eine rechtliche Grundlage von Nöten. Diese kann sich

---

[7] **sog. Tracking**
[8] **sog. Opt-out**

aus dem Gesetz, einer ggf. kollektiven Regelung (Betriebsvereinbarung, Tarifvertrag), dem berechtigten nachzuweisenden Interesse der Verantwortliche Stelle oder der gesonderten Einwilligung des Mitarbeiters ergeben.

2.2 Datenverarbeitung aufgrund gesetzlicher oder kollektivrechtlicher Erlaubnis

Eine Datenverarbeitung ist immer dann zulässig, wenn diese aufgrund staatlicher Vorschriften verlangt, vorausgesetzt oder aber gestattet ist. Dabei müssen die Art und der Umfang der gesetzlich zulässigen Verarbeitung auch erforderlich sein und sich nach den staatlichen Vorschriften richten. Räumen diese einen sogenannten Handlungsspielraum ein, sind die schutzwürdigen Interessen des betroffenen Mitarbeiters hinreichend zu beachten.

Grundsätzlich findet die Datenverarbeitung zum Zwecke der Vertragsabwicklung statt. Eine über diesen Zweck hinausgehende Verarbeitung ist ebenfalls zulässig, wenn sie durch kollektivrechtliche Vorschriften (also Regelungen) erlaubt ist. Diese kollektivrechtlichen Regelungen (etwa ein Tarifvertrag) müssen jedoch den konkreten Verarbeitungszweck regeln.

2.3 Einwilligung in die Verarbeitung von Daten

Eine weitere Möglichkeit der Datenverarbeitung bildet die Einwilligung des Betroffenen Mitarbeiters. Diese Einwilligung ist nur freiwillig zu erklären. Jede Erklärung die deren Unfreiwilligkeit vermuten lässt, führt zur Unwirksamkeit der Einwilligungserklärung.

Schon aus beweisrechtlichen Gründen ist die Einwilligung schriftlich (iSv. § 126 BGB) einzuholen. Sie kann jedoch auch in elektronischer Form (iSv. 126 a BGB) erfolgen. Nur wenn im Einzelfall beide Varianten nicht durchführbar sind, wäre eine mündliche Einwilligung denkbar. Gleichwohl besteht auch in einem solchen Fall eine Pflicht zur ordnungsgemäßen Dokumentation. Schreiben nationale Vorschriften keine Einwilligung vor und gibt der Betroffene seine Daten freiwillig an, ist eine Einwilligung anzunehmen. Der Betroffene ist vor der Einwilligung gemäß IV.3. Datenschutzrichtlinie transparent zu informieren.

2.4 Verarbeitung von Daten wegen eines berechtigten Interesses

Besteht für die Verantwortliche Stelle ein berechtigtes Interesse, so kann eine Verarbeitung personenbezogener Daten ebenfalls erfolgen. Unter einem berechtigten Interesse versteht man rechtlich oder wirtschaftlich tragende Gründe.

Zu den rechtlichen Gründen zählen insbesondere die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche, zu den wirtschaftlichen beispielsweise die Bewertung des Unternehmens.

Ergeben sich im Einzelfall Indizien für ein schutzwürdigeres Interesse eines Mitarbeiters, so darf trotz des berechtigten Interesses der Verantwortlichen Stelle eine Verar-

beitung personenbezogener Daten nicht erfolgen. Dabei ist die Feststellung des schutzwürdigeren Interesses je Verarbeitungsvorgang vorzunehmen.

Die Verarbeitung von Mitarbeiterdaten im Rahmen von Kontrollmaßnahmen darf nur bei einer gesetzlichen Verpflichtung oder einem begründeten Anlass dazu erfolgen. Bei letzterem ist gleichwohl eine Verhältnismäßigkeitsprüfung der Kontrollmaßnahme durchzuführen. Dabei müssen die berechtigten Interessen des Unternehmens an der Kontrollmaßnahme (bspw. unternehmensinterne Regelungen, rechtliche Vorgaben) gegen die schutzwürdigen Interessen des Mitarbeiters am Ausschluss der Maßnahme in Abwägung gebracht werden. Nur wenn diese Abwägung zu einem Überwiegen der berechtigten Interessen des Unternehmens führt, ist die Verarbeitung der Mitarbeiterdaten angemessen (steht also im richtigen Verhältnis). Deshalb sind bereits vor jeder Maßnahme die Interessen beider Seiten zu dokumentieren. Auch sind eventuell bestehende Mitbestimmungs- und Informationsrechte (weitergehende Rechte) der Betroffenen zu berücksichtigen.

2.5 Verarbeitung besonders schutzwürdiger Daten

Eine Verarbeitung besonders schutzwürdiger Daten darf nur unter ganz bestimmten Voraussetzungen erfolgen. Besonders schutzwürdige Daten sind definiert als Daten über Gesundheit und Sexualleben, politische Meinung, rassische und ethnische Herkunft, über Gewerkschaftszugehörigkeit, über religiöse oder philosophische Überzeugung des Betroffenen. Dabei ist eine inhaltliche Auslegung dieser Begriffe im Lichte des BDSG-neu vorzunehmen, soweit sie im diesem Gesetz explizit geregelt. Mithin kann das deutsche Recht auch noch weitere Datenkategorien als besonders schutzwürdig einstufen. Eine Verarbeitung von Daten im Zusammenhang mit Straftaten ist möglich, unterfällt aber meistens besonderen Voraussetzungen des deutschen Rechtes (bspw. der Strafprozessordnung).

Das deutsche Recht muss eine Verarbeitung besonders schutzwürdiger Daten explizit vorschreiben oder erlauben. Eine Verarbeitung der verantwortlichen Stelle kann jedoch auch notwendig sein, um gewissen arbeitsrechtlichen Rechten und Pflichten im Verhältnis der Verantwortlichen Stelle zu ihren Mitarbeiterinnen und Mitarbeitern gerecht zu werden. Diesen ist es im Übrigen unbenommen, freiwillig und ausdrücklich in eine Verarbeitung einzuwilligen.

Bei geplanten Verarbeitungen besonders schutzwürdiger Daten, ist zuvor der Unternehmensbeauftragte für den Datenschutz zu informieren.

2.6 Neue Medien und Telekommunikation

Das Internet, die Telefonanlage(n) und die E-Mail-Adressen als auch der Auftritt in sozialen Netzwerken werden in erster Linie im Rahmen der betrieblichen Aufgabenstellungdurch durch die Verantwortliche Stelle zur Verfügung gestellt. Deshalb handelt es sich dabei auch um sogenannte *Arbeitsmittel* und *Unternehmensressource.* Den Rahmen ihrer Nutzung bestimmt das geltende Recht und die unternehmensinterne IT-Richtlinie bzw. Betriebsordnung. Ist die private Nutzung erlaubt, so sind, soweit ein-

schlägig, insbesondere das Telekommunikationsgesetz und das Fernmeldegeheimnis zu beachten.

Die Verantwortliche Stelle überwacht die genannten *Arbeitsmittel* nicht generell. Gleichwohl können zur Abwehr von Angriffen auf die unternehmenseigene IT-Infrastruktur Schutzmechanismen an den Übergängen ins das Unternehmens-Netz implementiert werden, mithin Muster von Angriffen analysiert und technisch störende bzw. schädigende Inhalte blockiert werden.

Zudem kann es zu einer zeitlich befristeten Protokollierung der Nutzung des Intranets und Internets, der E-Mail-Adressen, der Telefonanlage(n) und der internen sozialen Netzwerke kommen.

Davon zu trennen ist die personenbezogene Datenauswertung. Diese erfolgt nur bei einem konkreten Verdacht eines Gesetzes- (bspw. §§ 202a, 202 b., 303 b StGB) oder Richtlinienverstoßes (IT-Richtlinie, Betriebsordnung der Verantwortliche Stelle). Eine Kontrollmaßnahme durch den ermittelnden Bereich erfolgt stets entlang des Verhältnismäßigkeitsprinzips und unter Wahrung des deutschen Gesetzes sowie der hierzu getroffenen Regelungen (Compliance-System) der Verantwortlichen Stelle.

VI. Personenbezogene Daten im Rahmen der Übermittlung

Die Übermittlung personenbezogener Daten an einen unternehmensinternen oder aber externen Empfänger erfolgt nur unter Beachtung der in V. dieser Datenschutzrichtlinie geschilderten Voraussetzungen. Bevor es zur Übermittlung kommt, wird der Empfänger auf die ausschließliche Verwendung des bereits bei Erhebung festgelegten Zwecks verpflichtet.

Werden die Daten an einen Empfänger in einem Drittstaat[9] übermittelt, ist vorher sicherzustellen, dass ein mit dieser Datenschutzrichtlinie gleichartiger Datenschutz gewährleistet ist. Erfolgt die Übermittlung aufgrund gesetzlicher Verpflichtungen (bspw. Beibringung in grenzüberschreitenden steuerstrafrechtlichen Ermittlungsverfahren) eines Drittstaates, ist dies auch ohne vorherige Sicherstellung eines gleichwertigen Datenschutzniveaus möglich.

Für die Übermittlung von Daten durch Dritte an die Verantwortliche Stelle (bspw. Poolgesellschaft, IT-Entwicklungsgesellschaft, Inkassogesellschaft) ist es wichtig, dass zuvor sichergestellt ist, dass die Daten überhaupt für die vorgesehenen Zwecke verwendet werden dürfen.

VII. Auftragsverarbeitung (AV)

Wird ein Auftragnehmer durch einen Auftraggeber mit der Verarbeitung personenbezogener Daten beauftragt, ohne zugleich im Obligo für den dazugehörigen Geschäftsprozess zu stehen, liegt eine Auftragsdatenverarbeitung (kurz: ADV) vor. Das beauftragende Unter-

[9] **Vgl. XV.**

nehmen (Auftraggeber) behält dabei immer die volle Durchführungsverantwortung (bleibt also Verantwortlicher im Sinne des BDSG-neu bzw. der DS-GVO).

Kommt es zur Erteilung des Auftrags einer Datenverarbeitung (ADV), so sind die folgenden Anforderungen durch den jeweiligen Auftraggeber einzuhalten und noch während der Auftragsverarbeitung zu gewährleisten:

1. **Zunächst einmal hat der Auftragnehmer seiner Eignung entsprechend die erforderlichen technischen (Privacy by Design) und organisatorischen (Privacy by Default) Schutzmaßnahmen sicherzustellen.**
2. **Der Auftrag zur Datenverarbeitung ist in Textform (§126 b BGB) oder digital dem Auftragnehmer zu erteilen.**
   Mithin hat eine Dokumentation über die erteilten Weisungen des Auftraggebers zur Auftragsdatenverarbeitung sowie den Verantwortlichkeiten von Auftraggeber und Auftragnehmer zu erfolgen.
3. **Sämtliche vom Datenschutzbeauftragten der Verantwortlichen Stelle auf- bzw. bereitgestellten Vertragsstandards sind einzuhalten.**
4. **Vor dem Beginn der Auftragsdatenverarbeitung durch den Auftragnehmer, muss der Auftraggeber sicherstellen, dass die Pflichten des Auftragnehmers eingehalten werden. Diese Einhaltung kann der Auftragnehmer durch eine Zertifizierung dokumentieren. Eine Kontrolle dieser Einhaltung wird abhängig vom Risiko der Datenverarbeitung während der vertraglichen Laufzeit wiederholt.**
5. **Werden Auftragsdaten grenzüberschreitend verarbeitet, sind die nationalen Vorschriften zur Weitergabe personenbezogener Daten ins Ausland einzuhalten. Beispielsweise dürfen Transferierungen (z.B. Serverdienste) von persönlichen Daten aus der EU in einen Drittstaat nur bei Sicherstellung des Datenschutzniveaus der EU im jeweiligen Drittstaat des Auftragsnehmers stattfinden. Um dieses vergleichbare Datenschutzniveau zu sichern, gibt es folgende geeignete Maßnahmen:**

   a. **Die Verwendung der EU-Standartvertragsklauseln zur Auftragsdatenverarbeitung zwischen Drittstaat Auftragsnehmer und der Verantwortliche Stelle (von EU-Kommission offiziell verabschiedetes Vertragsmuster finden Sie unter: http://ec.europa.eu/justice/data-protection/international-transfer/transfer/index_en.htm)**

   b. **Die Teilnahme des Auftragsnehmers (Verarbeiters) an der sogenannten EU anerkannten Privacy-Shield-Zertifizierung und Vorlage dieses Nachweises gegenüber der Verantwortlichen Stelle (als Auftraggeber).**

   c. **Die für die Verantwortliche Stelle zuständige Datenschutzaufsichtsbehörde (Der Hessische Datenschutzbeauftragte Postfach 3163, 65021 Wiesbaden) erkennt die verbindlichen Unternehmensregeln des Auftragnehmers im Drittstaat als ausreichend an.**

VIII. Der Betroffene und seine Rechte

Macht der Betroffene von seinen nun folgenden Rechten Gebrauch, so trifft die Verantwortliche Stelle (bzw. deren jeweilig verantwortlichen Bereich) eine umgehende Bearbeitungspflicht, die zu keinerlei Nachteilen für den Betroffenen führen darf.

1. **Zunächst kann der Betroffene Auskunft darüber verlangen, welche personenbezogenen Daten über ihn gespeichert wurden, woher diese Daten stammen und zu welchem Zweck sie gespeichert werden. Die spezielleren Auskunftsrechte im Arbeitsrecht (bspw. das Einsichtsrecht in die Personalakte) bestehen davon unabhängig und darüberhinausgehend fort.**

2. **Kommt es zur Übermittlung von Daten an Dritte, so ist über die Identität des Empfängers sowie die Kategorien von Empfängern Auskunft zu erteilen.**

3. **Dem Betroffenen steht ein Recht auf Berichtigung bzw. Ergänzung seiner personenbezogenen Daten zu, wenn diese unvollständig oder gar unrichtig gespeichert sind.**

4. **Dem Betroffenen steht ein Widerspruchsrecht bezogen auf die Verwendung seiner personenbezogenen Daten zu Zwecken der Werbung oder Markt- und Meinungsforschung zu. Die Daten müssen für diese Zwecke nach Art. 18 DSGVO gesperrt werden.**

5. **Darüber hinaus ist der Betroffene berechtigt, sein *„Recht auf Vergessenwerden"* geltend zu machen, also die Löschung der gespeicherten personenbezogenen Daten zu verlangen, soweit dies gesetzlich vorgeschrieben ist. Den Rahmen dazu bildet Art. 17 DSGVO. Wonach u.a. dann zu löschen ist, wenn es an einer Rechtsgrundlage für die Verarbeitung fehlt bzw. diese weggefallen ist oder aber der Zweck der Verarbeitung (durch Zeitablauf) entfallen ist. Wichtig ist, dass der Löschung sogenannte Aufbewahrungspflichten entgegenstehen und diese den schutzwürdigen Interessen des Betroffenen im Falle einer Kollision möglicherweise vorgehen.**

6. **Abschließend hat der Betroffene ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, soweit sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation den Interessen an einer Verarbeitung der Verantwortlichen Stelle im jeweiligen Einzelfall vorgeht. Besteht eine Rechtspflicht zur Durchführung der Verarbeitung so kann auch ein Überwiegen der besonderen persönlichen Situation, nicht eine Verarbeitung durch die Verantwortliche Stelle verhindern und oder gar zum Löschen verpflichten.**

Information über Ihr Widerspruchsrecht nach Artikel 21 EU-Datenschutz-Grundverordnung (DSGVO)

1. Einzelfallbezogenes Widerspruchsrecht
Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Abs. 1 e DSGVO (Datenverarbeitung im öffentlichen Interesse) und Artikel 6 Abs. 1 f DSGVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Artikel 4 Abs. 4 DSGVO.
Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

2. Widerspruchsrecht gegen Verarbeitung von Daten zu Werbezwecken
In Einzelfällen verarbeiten wir Ihre personenbezogenen Daten, um Direktwerbung zu betreiben. Sie haben das Recht, jederzeit Widerspruch gegen die Verarbeitung Sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Der Widerspruch kann *formfrei* erfolgen und sollte möglichst telefonisch gerichtet werden an: +49 (0) ...

Unabhängig davon kann der Betroffene die ihm eingeräumten Rechte aus den Ziffern III, IV., V., VI., IX., X. und XIV. als *begünstigter Dritter* geltend machen.

Zur Durchsetzung Ihres Auskunftsrechtes kontaktieren Sie uns bitte per Mail, Fax oder Telefon.

Gerne kommen wir nach Ihrer Anfrage umgehend auf Sie zu und erklären uns Ihnen gegenüber zu den Ziffern VIII. 1. Bis 6.

IX. Die Verarbeitung ist vertraulich

Das Datengeheimnis (die Verpflichtung zur Vertraulichkeit) erstreckt sich auch auf personenbezogene Daten. Die unbefugte Erhebung, Nutzung oder Verarbeitung ist allen Mitarbeitern der Verantwortlichen Stelle strikt verboten. Unter „unbefugt" versteht man, die Verarbeitung der Daten durch einen Mitarbeiter, ohne, dass ihm dies zur Erfüllung seiner Aufgaben notwendig ist.

In diesem Zusammenhang gilt das sogenannte *Need-to-know-Prinzip*, welches bedeutet, dass Mitarbeiter nur soweit Zugang zu personenbezogenen Daten haben dürfen, wie dies zur Erfüllung ihrer jeweiligen Aufgaben erforderlich[10] ist. Erforderlich ist dafür ein sogenanntes Berechtigungskonzept des Unternehmens durch das die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten (ähnlich einem Fachbereichsorganigramm) aber auch deren Umsetzung und Pflege klar und transparent geregelt ist.

[10] **D.h.: Aufgabenerfüllung kann nicht anders und gleich geeignet als durch den Zugriff auf die personenbezogenen Daten erfüllt werden.**

Zu privaten oder rein wirtschaftlichen Zwecken dürfen Mitarbeiter personenbezogene Daten nicht nutzen, an unbefugte Personen übermitteln oder diese anderweitig zugänglich machen. Deshalb sind Mitarbeiter auch bei Beginn des Beschäftigungsverhältnisses durch den Arbeitgeber auf die Vertraulichkeit der Daten schriftlich zu verpflichten. Die Verantwortliche Stelle nimmt dies sehr ernst und hat eine solche Verpflichtungserklärung schon seit langem intern von allen Beschäftigten eingefordert.

Abschließend ist zu beachten, dass auch nach Beendigung des Beschäftigungsverhältnisses die Verpflichtung (des dann ehemaligen Beschäftigten) zur Vertraulichkeit der Daten fortbesteht.

X. Verarbeitungssicherheit

Getragen von dem Gedanken der bestmöglichen Sicherheit der Datenverarbeitung, sind personenbezogene Daten zu jeder Zeit vor dem unberechtigten Zugriff, der unrechtmäßigen Verarbeitung bzw. deren Weitergabe sowie gegen Verfälschung und Verlust oder gar Zerstörung zu schützen. Ob die Verarbeitung in Papierform oder aber elektronisch erfolgt spielt keine Rolle.

Bereits vor der Einführung neuer Datenverarbeitungsverfahren, namentlich neuer IT-Systeme im Rahmen technischer Umstellungen innerhalb der Verantwortlichen Stelle, sind die technisch[11] und organisatorischen[12] Maßnahmen zum Schutz personenbezogener Daten festzulegen und zu implementieren.

Die Parameter an denen sich diese Maßnahmen zu orientieren haben, sind:

- **Der jeweilige Stand der Technik,**
- **dem von der Verarbeitung ausgehenden Risiko sowie**
- **dem Schutzbedarf[13] der Daten.**

Jeder verantwortliche Fachbereich kann dazu den ext. Datenschutzbeauftragten bzw. IT-Sicherheitsbeauftragen oder aber den (soweit vorhandenen) Informationssicherheitsbeauftragten (ISO - Information Security Officer) zu Rate ziehen.

Die obig erwähnten technisch-organisatorischen Maßnahmen des Schutzes personenbezogener Daten verstehen sich als Teil eines Datenschutzsicherheitsmanagements der Verantwortlichen Stelle und unterliegen der ständigen Anpassung an technische und organisatorische Entwicklungen

XI. Interne und externe Datenschutzkontrolle

Die Verantwortliche Stelle führt regelmäßig sogenannte Datenschutzaudits (Überprüfungen) durch ausgewiesene externe Fachleute bzw. (Fach-)Anwälte für IT-Recht durch. Ziel

[11] **Privacy by Design**
[12] **Privacy by Default**
[13] **Durch Prozess zur Informationsklassifizierung ermittelt.**

der weiteren Kontrollen ist es DS-GVO- und BDSG-neu-*compliant* aufgestellt zu sein, denn Datenschutz ist uns ausweislich auch unserer aufgestellten Unternehmensgrundsätze sehr wichtig.

Die Durchführung dieser Audits wird durch unsere Verantwortlichen bzw. durch auf das Datenschutz-Prüfwesen spezialisierte ext. Fachinformatiker und (Fach-)Anwälte für IT-Recht koordiniert und betreut. Alle Ergebnisse und Auswertungen dieser Audits werden den Verantwortlichen bzw. IT-Sicherheitsbeauftragten der Verantwortlichen Stelle gemeldet.

Der zuständigen Datenschutzaufsichtsbehörde (Der Hessische Datenschutzbeauftragte Postfach 3163, 65021 Wiesbaden) wird auf Antrag hin, das jeweilige Ergebnis dieser Datenschutzkontrollen zur Aufsicht übermittelt.

Gleichwohl ist es der zuständigen Datenschutzaufsichtsbehörde unbenommen eigene Audits (Überprüfungen) im gesetzlich abgesteckten Rahmen bei der Verantwortlichen Stelle (Neo Consult GmbH & Co. KG, Wilhlemstraße 17, 35037 Marburg) zwecks Prüfung der Einhaltung dieser Datenschutzrichtlinie vorzunehmen.

XII. Datenschutzzwischenfälle

Alle Beschäftigten der Verantwortlichen Stelle sind dazu angehalten sich der besonderen Bedeutung des Datenschutzes bewusst zu sein. Auch deshalb fordert und fördert die Verantwortliche Stelle von ihren Beschäftigten, wahrgenommene Datenschutzverstöße bzw. Verstöße gegen diese Datenschutzrichtlinie unverzüglich dem jeweils Vorgesetzten (bzw. Weisungsbefugten) zu melden. Die jeweilige Vorgesetztenperson hat den Datenschutzverstoß unverzüglich der Verantwortlichen Stelle zu melden.

In den folgenden drei Fällen, die wir hervorheben möchten, sind vorgesehene Meldungen als Teil des *Information Security Incedent Managements (kurz: ITIL)* innerhalb der Verantwortlichen Stelle unverzüglich vorzunehmen, um den Meldepflichten des Unternehmens nach dem Recht der Bundesrepublik Deutschland nachkommen zu können.

Den drei erwähnten Fällen werden zugeordnet:

1. **die erfolgte unrechtmäßige Übermittlung personenbezogener Daten an Dritte,**
2. **der unrechtmäßige Zugriff durch einen Dritten auf personenbezogene Daten oder**
3. **der schlichte Verlust personenbezogener Daten.**

XIII. Verantwortlichkeiten und Sanktionen bei Verstößen

Die Geschäftsführung der Verantwortlichen Stelle ist in ihrem (gesetzlich definierten) Verantwortungsbereich für die Datenverarbeitung verantwortlich. Aus ihrer Stellung heraus erwächst die Verpflichtung zur Sicherstellung der gesetzlichen und derjenigen Vorgaben, die in dieser Datenschutzrichtlinie genannt sind. So haben sie beispielsweise der Meldepflicht des Art. 33 DS-GVO nachzukommen. Deshalb obliegt Ihnen auch die Managementaufgabe, durch organisatorische, personelle und technische Maßnahmen sicherzustellen,

dass eine ordnungsgemäße Datenverarbeitung unter Einhaltung der gesetzlichen Vorschriften erfolgt.

Die konkrete Umsetzung der durch die Geschäftsführung aufgestellten Grundsätze obliegt dagegen den zuständigen Mitarbeitern in den Abteilungen.

Kommt es zu Datenschutzkontrollen der zuständigen Datenschutzbehörde (Der Hessische Datenschutzbeauftragte Postfach 3163, 65021 Wiesbaden), so ist die Verantwortlichen Stelle umgehend darüber in Kenntnis zu setzen.

Die Geschäftsführung ist dazu verpflichtet den Datenschutzbeauftragten in seiner Tätigkeit vollumfänglich zu unterstützen und in den Optimierungsprozessen zu fördern.

Bei Verarbeitungsvorgängen, aus denen besondere Risiken für die Persönlichkeitsrechte des Betroffenen erwachsen, ist schon vor Beginn der Verarbeitung Kontakt zum Datenschutzbeauftragten der Verantwortlichen Stelle aufzunehmen. Dies ist namentlich bei besonders schutzwürdigen personenbezogenen Daten der Fall.

Die Verantwortliche Stelle hat sicherzustellen, dass sämtliche Mitarbeiter zum Thema des Datenschutzes geschult sind und auch auf dem aktuellen Stand bleiben.

Missbrauch bei der Datenverarbeitung kann - wenn Vorsatz oder Fahrlässigkeit gegeben sind - gegebenenfalls über eine Ordnungs- bzw. Datenschutzwidrigkeit hinaus auch strafrechtliche Relevanz entfalten. Die Verantwortliche Stelle nimmt das gesamte Thema *„Schutz der eigenen Daten“* als hohes Rechtsgut sehr ernst. Die Verantwortliche Stelle stellt diese Einstellung zum Datenschutz u.a. durch eine reibungslose Kommunikation und Zusammenarbeit mit den Strafjustizbehörden in Datenmissbrauchsfällen auch unter Beweis.

Der Datenmissbrauch durch eigene Mitarbeiter wird nicht toleriert und - soweit nachweisbar - mit arbeitsrechtlichen Konsequenzen überzogen.

XIV. Definitionen

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

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

***Besonders schutzwürdige Daten* sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse und philosophische Überzeugungen, über eine Gewerkschaftszugehörigkeit oder über die Gesundheit oder die sexuelle Orientierung des Betroffenen. Aufgrund des nationalen Rechts der Bundesrepublik Deutschland sind diese Datenkategorien als besonders schutzwürdig eingestuft.**

Betroffener **im Sinne dieser Datenschutzrichtlinie ist jede natürliche Person, über die Daten verarbeitet werden.**

Verantwortlicher **ist die jeweilige Gesellschaft der Verantwortlichen Stelle, deren Geschäftliche Aktivität die jeweilige Maßnahme einer Verarbeitung nach sich zieht.**

Einwilligung **ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.**

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

Übermittlung **ist jede Weitergabe bzw. die Kommunikation von geschützten Daten durch den Verantwortlichen an Dritte.**