PRIVACY - DATENSCHUTZ (D. Lgs. 196 vom 30.06.2003)

Mit diesem Informationsblatt soll ein Überblick zu den Maßnahmen betreffend Datenschutz gegeben werden. Im **Anhang (Punkt 9)** finden Sie, für ein besseres Verständnis der Begriffe, die dazugehörigen Definitionen.

1) WER IST VON DIESEM GESETZ BETROFFEN?

Die Bestimmungen gelten für Privatpersonen, Unternehmer, Freiberufler, Personen- und Kapitalgesellschaften und private sowie öffentliche Körperschaften, die in irgendeiner Form (z. B. mit Computer oder auf Papier) persönliche Daten von anderen Personen im italienischen Staats- bzw. Hoheitsgebiet verwalten und verarbeiten.

2) ANDERE FIRMEN SENDEN MIR AUFKLÄRUNGSCHREIBEN (INFORMATIVA) ZU, MUSS ICH DIESE UNTERSCHREIBEN BZW. MEINE EINWILLIGUNG GEBEN?

Diese Aufklärungsschreiben müssen nur unterschrieben und an den Absender zurückgesendet werden, wenn es für die Einwilligung keine Befreiung (siehe unter Punkt 4) von Seiten der Datenschutzbehörde gibt.

In jedem Fall ist die **Einwilligung** und somit die Unterschrift zu leisten, wenn es sich um die Verarbeitung von **sensiblen Daten bzw. Gerichtsdaten handelt**.

3) MUSS ICH DAS AUFKLÄRUNGSSCHREIBEN (INFORMATIVA) AN MEINE GESCHÄFTSPARTNER SCHICKEN?

Der Betroffene (also die Personen, auf die sich die verarbeiteten Daten beziehen) muss vor Beginn der Datenverarbeitung über folgende Aspekte informiert werden:

- Ziele und Form der Datenverarbeitung;
- die Rechtspersonen bzw. Kategorien von Rechtspersonen, denen die Daten mitgeteilt werden können und die Bereiche, in denen die Daten verbreitet werden können;
- seine Rechte (z. B. die Aktualisierung, Berichtigung und Löschung von Daten sowie die Verweigerung der Einwilligung und deren Konsequenzen);
- den Namen des Rechtsinhabers und zumindest eines Verantwortlichen für den Datenschutz.

Dies kann folgendermaßen erfolgen:

a) **Mündlich:** das Gesetz sieht vor, dass der Betroffene mündlich aufgeklärt werden kann, in der Praxis ist das wahrscheinlich sehr zeitaufwendig und im Falle eines Rechtsstreits schwierig zu beweisen

b) **Schriftlich:** man schreibt an die betroffenen Personen einen Brief, Email, Fax, wo die oben angeführten Informationen enthalten sind

c) **Internet:** das Aufklärungsschreiben kann auch auf der Internetseite des Unternehmens veröffentlicht werden; es genügt dann ein Hinweis auf diese Internetseite auf dem Schriftverkehr des Unternehmens (z. B. auf den Rechnungen, Lieferscheinen, Email, Briefpapier, Fax ...).

Unser Vorschlag für eine möglich Formulierung:
„Ihre Daten werden im Sinne des Gesetzesvertretenden Dekretes vom 30.06.03 Nr.196 (Datenschutzkodex) verarbeitet.
Die vollständige Aufklärung, sowie die Rechte des Betroffenen sind auf unserer Website: http://www._____ abzurufen."
"I Vostri dati vengono elaborati secondo il Dlgs 30 giugno 2003 nr. 196 (Codice della Privacy).

L'informativa relativa il trattamento dei dati personali, e tutti i diritti dell'interessato sono pubblicati sul nostro sito web: http://www._____"

4) WANN BIN ICH VON DER EINHOLUNG DER EINWILLIGUNG BEIM BETROFFENEN BEFREIT?

Die Datenschutzbehörde hat in verschiedenen Verordnungen und Erläuterungen Erleichterungen für die Einwilligung eingeführt. So ist die **Einwilligung** des Betroffenen **nicht erforderlich**, **wenn** es sich beispielsweise um:

- Daten, die auf der Grundlage gesetzlicher Vorschriften (des nationalen wie des EU-Gesetzgebers) gesammelt bzw. verwaltet werden;
- Verarbeitungen, die notwendig sind, um Verpflichtungen aus einem Vertrag zu erfüllen (dazu zählen auch die **Kunden- und Lieferantendaten**, sofern nicht auch sensible bzw. Gerichtsdaten verwaltet werden);
- Daten, die aus öffentlichen Registern und Verzeichnissen sowie aus allgemein zugänglichen bzw. einsehbaren Urkunden oder Dokumenten entnommen werden;
- Daten, die sich – unter Beachtung der Gesetze zum Schutz des geistigen Eigentums - auf die Ausübung einer wirtschaftlichen Tätigkeit beziehen;
- die Verarbeitung von Daten zum Zwecke der Geltendmachung von Rechten in einem Gerichtsverfahren;
- die Verarbeitung von Daten durch Vereinigungen, Körperschaften und Organisationen ohne Gewinnabsicht, sofern die Betroffenen mit ebendiesen Rechtspersonen regelmäßigen Kontakt pflegen oder aber Mitglieder sind und die Verarbeitung zu institutionellen Zwecken erfolgt (z. B. Unternehmerverband; LVH; HGV; VKD; Onlus und Volontariatsvereine, normalerweise Vereine im allgemeinen u. a.);

handelt.

In all diesen Fällen besteht somit keine Verpflichtung eine schriftliche Einwilligung beim Betroffenen einzuholen.

Die Einwilligung bei der Verwaltung von sensiblen Daten bzw. Gerichtsdaten ist hingegen immer erforderlich.

5) WANN MUSS ICH EINE MITTEILUNG AN DIE DATENSCHUTZBEHÖRDE MACHEN?

Eine Mitteilung an die Datenschutzbehörde ist nach den neuen Bestimmungen im allgemeinen nur mehr dann zu machen, wenn nachfolgende Daten verarbeitet werden und es dafür **keine Standardermächtigung** von Seiten der Datenschutzbehörde gibt:

- **Sensible Daten** (Als sensible Daten gelten Daten, welche die rassische oder ethnische Herkunft; die religiöse, philosophische oder andere Weltanschauung; die politische Anschauung, die Mitgliedschaft in einer Partei, Gewerkschaft, Vereinigung oder Organisation mit religiöser, philosophischer, politischer oder gewerkschaftlicher Ausrichtung; den Gesundheitszustand bzw. Krankheiten oder das Sexualleben einer Person erkennen lassen)
- **Gerichtsdaten**
- Informationen zur Bonität, Vermögenssituation, zur korrekten Erfüllung von Verpflichtungen sowie zu betrügerischen oder allgemein gesetzeswidrigem Handlungen, die in eigenen elektronischen Datenbanken gespeichert werden

Sogenannte „**Standardermächtigungen**" gibt es zur Zeit für

- „Sensible" Daten, die sich auf ein Arbeitsverhältnis beziehen;
- Daten zum Gesundheitszustand und zum Sexualleben;
- die Verarbeitung von „Sensiblen" Daten" durch Vereinigungen und Stiftungen;
- die Verarbeitung von „Sensiblen" Daten" durch Freiberufler;
- die Verarbeitung von „Sensiblen" Daten" durch Banken, SIM, Versicherungen, Datenverarbeitungsbetriebe, Tourismusbetriebe, Marktforschungsinstitute, Partnerschaftsinstitute, Personalberatungen etc.); Verarbeitung von „Sensiblen" Daten" durch Privatdetektive;
- Gerichtsdaten

und man ist somit von der **Mitteilung an die Datenschutzbehörde befreit**.

Die Mitteilung an die Datenschutzbehörde hat in **telematischer Form** auf den eigens dafür vorgesehenen **Vordrucken** (www.garanteprivacy.it) vor Beginn bzw. bei Änderung der Datenverarbeitungstätigkeit zu erfolgen.

6) MINDESTSICHERHEITSMASSNAHMEN (MISURE MINIME DI SICUREZZA) – WAS IST ZU TUN?

Grundsätzlich ist jeder (Firmen, Freiberufler, Vereine usw.), der persönliche Daten in irgendeiner Form verarbeitet, verpflichtet die Risiken im Zusammenhang mit folgende Ereignissen zu minimieren und zu regeln:

1. Zerstörung oder Verlust von Daten (auch unbeabsichtigt);
2. Nicht autorisierter Zugriff;
3. Unzulässige bzw. widerrechtliche Verarbeitung von Daten.

Diese Regelungen müssen jährlich aktualisiert werden.

Hinweis:
Es empfiehlt sich deshalb **diese Regelungen schriftlich festzuhalten**. Eine **Standardvorlage** können Sie diesbezüglich bei uns im Büro anfordern.

Man unterscheidet folgende Fälle:

6.1) VERARBEITUNG VON PERSÖNLICHEN DATEN OHNE ELEKTRONISCHE HILFSMITTEL

Es müssen folgende Maßnahmen ergriffen werden:

- Für jeden Datenverarbeitungsbeauftragten (siehe Definitionen) muss der Bereich der zugänglichen Daten und –Verarbeitungen definiert und mindestens einmal jährlich aktualisiert werden;
- Im Hinblick auf die Kontrolle und Aufbewahrung von Schriftstücken und Unterlagen mit personenbezogenen Daten müssen schriftliche Anweisungen erteilt werden; Schriftstücke und Unterlagen mit „sensiblen" oder Gerichtsdaten müssen so archiviert werden, dass Unbefugte keinen Zugriff haben;
- Der Zugriff auf Archive mit „sensiblen" bzw. Gerichtsdaten muss beaufsichtigt werden; Personen, die nach Büroschluss Zugang zu den Räumlichkeiten haben, müssen identifiziert und registriert werden; verfügen die Archive über keine elektronische Zugangskontrolle und werden sie nicht bewacht, so muss jeder Zugang vorher ermächtigt werden.

6.2) VERARBEITUNG VON PERSÖNLICHEN DATEN MIT ELEKTRONISCHEN HILFSMITTELN

Grundsätzlich müssen folgende Maßnahmen ergriffen werden (diese Aufzählung stellt eine vereinfachende Zusammenfassung dar):

- Für jeden Datenverarbeitungsbeauftragten (siehe Definitionen) und für jede Person, welche die elektronischen Hiflsmittel (z. B. Computer) benutzt oder wartet, muss der Bereich der zugänglichen Daten und –Verarbeitungen definiert und mindestens einmal jährlich aktualisiert werden; die **Beauftragung** des Beauftragten für die Datenverarbeitung (siehe Definition in Punkt 9) hat **schriftlich** zu erfolgen (**eine Standardformular für die Beauftragung kann bei uns im Büro angefordert werden**);
- Jedem Beauftragten muss ein Identifizierungscode (z.B. login, PIN, username) und ein Passwort aus zumindest 8 Zeichen (bzw. so viele, wie es das System gestattet) zugeordnet werden; das Passwort darf nicht in unmittelbarer bzw. offensichtlicher Beziehung zum Beauftragten stehen (z.B. der Vorname) und muss alle sechs Monate geändert werden;
- Verfällt der Status eines Beauftragten für die Datenverarbeitung, so muss für die betreffende Person der Zugang zu personenbezogenen Daten sofort unterbunden werden;
- Die Computer und die Daten müssen vor unbefugtem Zugriff und rechtswidrigen Verarbeitungen geschützt werden;
- Die Software muss jedes Jahr aktualisiert werden;
- Die Anti-Virus-Software muss alle sechs Monate aktualisiert werden;
- Eine Sicherstellung (Backup) der Daten muss zumindest einmal wöchentlich erfolgen; für die Aufbewahrung der Datenträger müssen angemessene Sicherheitsprozeduren festgelegt werden.

Die Implementierung dieser Maßnahmen muss durch Dritte (im Normalfall die Computerfirma) bestätigt werden (sog. Konformitätsbescheinigung).

6.3) VERARBEITUNG VON "SENSIBLEN" UND VON GERICHTSDATEN

Werden sensible Daten (siehe Definition unter Punkt 9) und/oder Gerichtsdaten verarbeitet, so sind **zusätzlich** zu den Maßnahmen in Punkt 6.2) noch folgende Maßnahmen erforderlich:

- Das Passwort muss alle drei Monate ersetzt werden;
- Die Software muss alle sechs Monate aktualisiert werden;
- Die Daten müssen gegen unbefugten Zugriff mit geeigneten elektronischen Instrumenten geschützt werden;
- Im Hinblick auf die Aufbewahrung und die Verwendung mobiler Datenträger (z.B. Floppy-Disks, CD, DVD, Bandsicherungen usw.) müssen organisatorische und technische Anweisungen an die Datenbeauftragten erteilt werden;
- Im Falle einer Beschädigung der Daten oder der Computer müssen geeignete Maßnahmen ergriffen werden, um diese wiederherzustellen;
- Das **Programmatische Dokument der Sicherheit** („**D.P.S.**" oder auch **Sicherheitsplan** genannt) (siehe Punkt 7) **muss jedes Jahr aktualisiert werden**.

7) PROGRAMMATISCHES DOKUMENT DER SICHERHEIT (D.P.S.: DOCUMENTO PROGRAMMATICO SULLA SICUREZZA)

Jeder der „**sensible Daten**" oder **Gerichtsdaten über Computer (EDV)** verarbeitet, ist innerhalb 31. März eines jeden Jahres verpflichtet, das „**Programmatische Dokument der Sicherheit**" (documento programmatico sulla sicurezza – DPS) zu erstellen bzw. zu aktualisieren (umfasst alle Maßnahmen unter 6.1) und 6.2)).

Das Programmatische Dokument der Sicherheit muss folgende Angaben enthalten:

- Liste der persönlichen Daten, die verwaltet werden;
- Verteilung von Aufgaben und Zuständigkeiten im Bereich Datenschutz;
- Risikoanalyse;
- Die erforderlichen Maßnahmen, um die Integrität und Verfügbarkeit der Daten zu gewährleisten und um die Räumlichkeiten zu schützen, in denen die Daten verwaltet werden;
- Kriterien und Modalitäten, um die Verfügbarkeit der Daten nach einem Schadensfall wiederherzustellen;
- Ausbildungsmaßnahmen für die Datenschutzbeauftragten;
- Kriterien, um die Einhaltung der Mindestsicherheitsmaßnahmen im Fall einer Auslagerung der Datenverwaltung zu gewährleisten;
- Schließlich ist anzugeben, wie die Informationen zum Gesundheitszustand und zum Sexualleben verschlüsselt oder aber gesondert von den übrigen personenbezogenen Daten verwaltet werden sollen.

Hinweis:
Ein **Standardmodell** für das „Programmatische Dokument der Sicherheit" kann von der Internetseite der Datenschutzbehörde heruntergeladen werden: „www.garanteprivacy.it –*facsimile e adempimenti – documento programmatico sulla sicurezza*".

Für kleinere Unternehmen mit einfachen EDV-Systemen kann dieses Standardmodell verwendet werden. Bei **komplexeren EDV-Systemen** empfehlen wir es sich einen **externen Berater** zuzuziehen bzw. mit dem **EDV-Lieferanten** Absprache zu halten, da dieser über die Hardware und Software genauestens Bescheid weis.

8) STRAFEN

Das neue Datenschutzgesetz sieht empfindliche Strafen für die Nichteinhaltung der Vorschriften vor. Die Verwaltungsstrafen liegen zwischen **3.000 Euro und 60.000 Euro**. Strafrechtlich werden die Vergehen mit Gefängnistrafen **von 6 Monaten bis zu 3 Jahren** geahndet.

9) DEFINITIONEN

Betroffener: der sog. Betroffene ist die natürliche oder juristische Person, auf die sich die persönlichen Daten beziehen.

Rechtsinhaber: der Rechtsinhaber ist die natürliche oder juristische Person, welche – auch gemeinsam mit anderen Inhabern – die Entscheidungsbefugnis im Hinblick auf die Ziele und Modalitäten der Datenverarbeitung, die Verwendung von Hilfsmitteln und eben den Schutz der verarbeiteten Daten innehat.
Gesellschaften bzw. Körperschaften sind in ihrer Gesamtheit Rechtsinhaber; naturgemäß sind es dann die Verwalter bzw. Rechtsvertreter, welche in der Ausübung ihrer Ämter auch für den Datenschutz verantwortlich sind.

Verantwortlicher für die Datenverarbeitung: der Verantwortliche für die Datenverarbeitung ist eine natürliche oder juristische Person, der vom Rechtsinhaber die Verantwortung für die Datenverarbeitung übertragen wird.

Es können mehrere Verantwortliche ernannt werden; sie müssen über die erforderliche Erfahrung, die Fähigkeiten und die Zuverlässigkeit verfügen, um die Einhaltung der Datenschutzbestimmungen gewährleisten zu können.
Die Aufgaben, die dem Verantwortlichen übertragen werden, müssen vom Rechtsinhaber in Schriftform detailliert angegeben werden; der Rechtsinhaber wacht - auch durch regelmäßige Kontrollen – über die Einhaltung seiner Anweisungen sowie der geltenden Gesetze.

Beauftragte für die Datenverarbeitung: die Beauftragten im Sinne der Datenschutzbestimmungen sind natürliche Personen, die vom Rechtsinhaber oder vom Verantwortlichen mit der Verarbeitung von personenbezogenen Daten betraut werden.
Es handelt sich dabei um jene Personen, die an Terminals oder auch in Archiven tätig sind und konkret die Sammlung, Verwaltung, Verarbeitung im engeren Sinn und schließlich Speicherung von personenbezogenen Daten vornehmen; sie unterliegen der Entscheidungsbefugnis des Rechtsinhabers oder Verantwortlichen für den Datenschutz und haben seinen Anweisungen Folge zu leisten. **Die Beauftragung erfolgt schriftlich** und muss die Art bzw. den Bereich der Datenverarbeitung genau regeln.

Verarbeitung personenbezogener Daten ("Verarbeitung"): jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.

Persönliche oder personenbezogene Daten: alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Sensible Daten: personenbezogene Daten, welche Auskunft über die ethische bzw. rassische Herkunft, über religiöse, philosophische oder andere Überzeugungen, über die politische Meinung, über die Angehörigkeit zu politischen Parteien, Gewerkschaften, Vereinigungen und Organisationen religiösen, philosophischen, politischen und gewerkschaftlichen Charakters, sowie die über den Gesundheitszustand und das Sexualleben geben.

Einwilligung der betroffenen Person: jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene bzw. sensible Daten, die sie betreffen, verarbeitet werden.