REGLEMENT PRIVACY

VERARBEITUNG PERSONEN- UND UNTERNEHMENSBEZOGENER DATEN

Art. 1 – Ziele der IDM zur Datenverarbeitung

Ziel des vorliegenden Reglements ist die Gewährleistung einer Datenverarbeitung innerhalb der Betriebstätigkeiten, welche die Rechte und Grundfreiheiten sowie die Würde der betroffenen Personen respektiert, mit besonderem Augenmerk auf Privatsphäre, die persönliche Identität und das Recht auf Datenschutz.

Die folgenden Vorschriften wurden gemäß dem Datenschutzkodex (GvD. 196/2003), den Verfügungen der Datenschutzbehörde und den Anforderungen des internationalen Standards ISO 27001 zur Informationssicherheit erstellt.

Art. 2 – Begriffsbestimmungen

Im Rahmen ihrer Betriebstätigkeit verarbeitet die IDM zwei Arten von Daten: personenbezogene Daten (geschützt vom GvD 196/ 2003 – Datenschutzkodex) und unternehmensbezogene Daten (geschützt von den Betriebsvorschriften).

Personenbezogene Daten sind alle Informationen über eine bestimmte oder auch nur indirekt bestimmbare natürliche Person durch Bezugnahme auf irgendeine andere Information, auch eine persönliche Kennnummer.

Sensible Daten sind personenbezogene Daten, welche Aufschluss über den Gesundheitszustand und das Sexualleben einer Person, ihre rassische und ethnische Herkunft, die religiöse, philosophische oder eine andere Weltanschauung, die politischen Anschauungen, die Mitgliedschaft bei einer Partei, Gewerkschaft, Vereinigung oder Organisation mit religiöser, philosophischer, politischer oder gewerkschaftlicher Ausrichtung geben können.

Gerichtsdaten sind personenbezogene Daten, die Aufschluss geben können über Verfügungen und Maßnahmen in Zusammenhang mit dem Strafregister, dem Register über anhängige Verwaltungs-

REGOLAMENTO PRIVACY

TRATTAMENTO DEI DATI PERSONALI E AZIENDALI

Art. 1 – Obiettivo IDM per il trattamento dei dati

Il presente Regolamento ha lo scopo di garantire che il trattamento dei dati nell'ambito dell'attività aziendale si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Le seguenti regole sono realizzate in conformità alle richieste previste dal Codice in materia di protezione dei dati personali (D.lgs. 196/2003 – Codice Privacy), dei Provvedimenti del Garante e dei requisiti di sicurezza delle informazioni dello standard internazionale ISO 27001.

Art. 2 - Definizioni

Nell'ambito delle attività di IDM vengono trattate due tipologie di dati: i dati personali (tutelati dal D.lgs. 196/2003 - Codice Privacy) ed i dati aziendali (tutelati dalle Regole aziendali).

I **dati personali** sono qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

I **dati sensibili** sono i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

I **dati giudiziari** sono i dati idonei a rilevare informazioni riguardo provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai

strafverfahren und die verhängten Verwaltungsstrafen oder über die Eigenschaft einer Person als Angeklagter oder als den Vorerhebungen unterworfene Person (Verdächtiger) im Sinne der Artikel 60 und 61 der Strafprozessordnung.

sensi degli articoli 60 e 61 del codice di procedura penale.

Die Verarbeitung von Daten, welche nicht zu den sensiblen Daten bzw. Gerichtsdaten gehören, aber aufgrund ihrer Natur und der Art und Weise sowie den Folgen der Verarbeitung spezifische Risiken in Zusammenhang mit den Rechten und Grundfreiheiten bzw. der Würde der betroffenen Personen mit sich bringen können (**besondere Daten**), ist nur unter Anwendung von eigenen Maßnahmen und Vorkehrungen zum Schutz der Betroffenen möglich.

Il trattamento dei dati diversi da quelli sensibili e giudiziari (**dati particolari**), che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

Die Verarbeitung personenbezogener Daten bezeichnet jeden auch ohne elektronische Mittel ausgeführten Vorgang oder jede Vorgangsreihe in Zusammenhang mit der Erhebung, Speicherung, Organisation, Aufbewahrung, Abfrage, Verarbeitung im engeren Sinn, Änderung, Auswahl, Auslese, Verleihung, Verwendung, Verknüpfung, Sperrung, Übermittlung, Verbreitung, Löschung und Vernichtung von Daten, auch wenn sie nicht in einer Datenbank gespeichert sind.

Il trattamento dei dati personali corrisponde a qualunque operazione o complesso di operazioni, effettuata anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

Die **Übermittlung von personenbezogenen Daten** besteht darin, dass personenbezogene Daten einem oder mehreren Außenstehenden – also Personen, die nicht die betroffene Person sind – in jedweder Form, auch durch Bereitstellen oder Bereithalten zur Abfrage, zugänglich gemacht werden.

La comunicazione di dati personali consiste nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

Die **Verbreitung von personenbezogenen Daten** besteht darin, dass personenbezogene Daten Außenstehenden, auch durch Bereitstellen oder Bereithalten zur Abfrage, zugänglich gemacht werden.

La diffusione di dati personali avviene quando viene data conoscenza dei dati personali a soggetti indeterminati in qualunque forma, anche mediante la loro messa disposizione o consultazione.

Rechtsinhaber der Datenverarbeitung ist die natürliche Person, juristische Person, öffentliche Verwaltung oder jede andere Körperschaft, Vereinigung oder Einrichtung, die das Recht hat, auch zusammen mit einem anderen Rechtsinhaber, über den Zweck der Verarbeitung personenbezogener Daten, über die jeweilige Verfahrensweise und über die dafür verwendeten Mittel, einschließlich der Datensicherung, zu entscheiden.

Il **Titolare del trattamento** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisione in ordine alle finalità, alle modalità del trattamento di dato personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Rechtsinhaber der Datenverarbeitung in der IDM ist der Präsident und gesetzliche Vertreter, Dr. Thomas Aichner.

Verantwortlicher der Datenverarbeitung bezeichnet die natürliche Person, welche vom Rechtsinhaber mit der Kontrolle der Verfahren und Modalitäten der Verarbeitung personenbezogener Daten betraut wird.

Verantwortliche der Datenverarbeitung in der IDM sind der Generaldirektor, Hansjörg Prast, die Direktoren der einzelnen Abteilungen sowie die Bereichsleiterin Human Resources.

Systemverwalter bezeichnet die natürliche Person, welche vom Rechtsinhaber mit der Sicherheitsüberprüfung des Computersystems betraut wird.

Systemverwalter in der IDM ist Herr Manfred Inama.

Datenverarbeitungsbeauftragter bezeichnet die natürliche Person, die vom Rechtsinhaber die Befugnis zur Datenverarbeitung gemäß den von der Organisation festgelegten Vorschriften erhält. Der Artikel 30 des Datenschutzkodex verfügt, dass Verarbeitungsvorgänge nur durch Beauftragte ausgeführt werden dürfen, die dem Rechtsinhaber oder Verantwortlichen direkt unterstellt sind und sich an deren Weisungen zu halten haben. Die Namhaftmachung der Beauftragten erfolgt schriftlich und beinhaltet jeweils den erlaubten Verarbeitungsbereich.

Betriebsdaten sind sämtliche betriebsbezogene Daten und Informationen (geordnet oder ungeordnet, in Papierform oder elektronischer Form), welche im Bereich der IDM verarbeitet werden, und sind Betriebseigentum und -vermögen der IDM. Betriebsbezogene Daten sind alle Daten und Informationen, die, einzeln oder in gesammelter Form, auch nur möglicherweise einen ungerechten Vorteil zugunsten unrechtmäßiger Dritter schaffen können.

Art. 3 – Räumlichkeiten und Arbeitsbereiche

Die Räumlichkeiten und sämtliche Arbeitsbereiche, in denen sich die Ausstattung der IDM befindet, müssen mit höchster Sorgfalt benutzt und bewahrt werden, um einen effizienten Arbeitsablauf und ein

Il Titolare del Trattamento dei dati per IDM è il Presidente e rappresentante legale, dott. Thomas Aichner.

Responsabile del trattamento è la persona fisica preposto dal Titolare al controllo delle procedure e modalità di trattamento dei dati personali.

I Responsabili del trattamento per IDM sono il Direttore generale, Hansjörg Prast, i Dirigenti delle singole ripartizioni nonché la Responsabile delle risorse umane.

Amministratore di sistema è la persona fisica preposta dal Titolare, cui spetta la gestione della sicurezza del sistema informatico.

L'Amministratore per la IDM è il sig. Manfred Inama.

Incaricato del trattamento è la persona fisica autorizzata a compiere operazioni di trattamento dati in base alle regole definite dall'organizzazione. L'articolo 30 del Codice Privacy dispone che le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione degli incaricati deve essere effettuata per iscritto, individuando puntualmente l'ambito del trattamento consentito.

I **dati aziendali** sono tutti i dati e le informazioni aziendali (strutturati o destrutturati, in formato cartaceo o digitale) trattati nell'ambito di IDM e rappresentano una proprietà aziendale, patrimonio di IDM. I dati aziendali sono tutti i dati e le informazioni che, singolarmente o in forma aggregata, possono procurare anche solo potenzialmente ingiusto vantaggio competitivo a favore di terzi non legittimati.

Art. 3 – Gestione dei locali e delle aree di lavoro

I locali e tutte le aree di lavoro comprensive di tutte le dotazioni di IDM devono essere utilizzate e custodite con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni.

angemessenes Sicherheitsniveau der Informationen zu gewährleisten.

Das gesamte beschäftigte Personal und sämtliche dritte Personen, welche mit der IDM zusammenarbeiten und Zugang zu den Räumlichkeiten und natürlichen Ressourcen haben, müssen sich an die Regelungen zur Gewährleistung der physischen Sicherheit von Arbeitsbereichen und Betriebsräumlichkeiten halten.

Tutto il personale dipendente e tutti i soggetti terzi che collaborano con IDM, aventi accesso ai locali e alle risorse fisiche, devono attenersi alle policy per garantire la sicurezza fisica di aree ed asset aziendali.

Art. 4 – Zutritt zu Büros und geschützten Bereichen

Der **Zutritt zu den Büroräumlichkeiten** ist nur ausdrücklich beauftragtem Personal gestattet, welches zu Arbeitszwecken Anspruch auf Zutritt zu den Räumlichkeiten hat.

Der **Zutritt zum Data Center** der IDM erfolgt ausschließlich unter Anwesenheit von befugtem IDM-Personal.

Der Gebrauch des **Arbeitsplatzes** und der damit einhergehende Zugang zu Dokumenten, Akten und Archiven ist im Rahmen der Funktion des Mitarbeiters und der ihm aufgetragenen Aufgaben erlaubt. Nach Abschluss des Arbeitstages und/oder bei Abwesenheit dürfen vertrauliche Dokumente und Akten, besonders jene, die Daten und Informationen sensibler und/oder vertraulicher Natur beinhalten, nicht offen liegen bleiben.

Art. 4 – Accesso agli uffici ed aree protette

L'**accesso agli uffici** è permesso solo a personale espressamente incaricato in base a precise e motivate esigenze connesse a finalità lavorative.

L'**accesso ai locali Data Center** di IDM è ammesso esclusivamente da parte di personale autorizzato.

L'utilizzo della **postazione di lavoro** e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi assegnati. Al termine della giornata lavorativa e durante eventuali periodi di assenza non devono essere lasciati visibili documenti e atti riservati, con particolare riferimento a quelli contenenti dati e informazioni di natura sensibile e/o riservati.

Art. 5 – Maßnahmen zur Verwahrung von Dokumenten und Akten in Papierform

Dokumente in Papierform, welche zur Ausführung der Arbeitstätigkeit benötigt werden, sind im jeweiligen Büro zu verwahren. Zu allen Archiven ist der Zutritt beschränkt und nur möglich, um Dokumente zu entnehmen und abzulegen, die für die Ausführung der Arbeitstätigkeit benötigt werden. Bei vorübergehender Abwesenheit und nach Abschluss der Arbeitstätigkeit im jeweiligen Bereich sind die Dokumente korrekt abzulegen. Falls die Notwendigkeit besteht, ein Dokument mit sensiblen Daten auf Papier zu drucken, darf das Dokument nur für den Zeitabschnitt verwendet werden, welcher für die Abwicklung der Aufgabe nötig ist. Danach ist das Dokument zu beseitigen.

Art. 5 – Modalità di custodia dei documenti e atti cartacei

I documenti cartacei necessari allo svolgimento delle mansioni lavorative devono essere custoditi nell'area del proprio ufficio. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi esclusivamente per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa nell'area di pertinenza. Quando vi sia l'esigenza di produrre la stampa di un documento contenente dati sensibili, questo dovrà essere mantenuto esclusivamente per il tempo strettamente necessario alla lavorazione della pratica, decorso il quale il documento dovrà essere fisicamente eliminato.

Dokumente und Akten mit sensiblen personenbezogenen oder Gerichtsdaten müssen in verschlossenen Archiven aufbewahrt werden.

Die Beseitigung jedes Dokumentes in Papierform, welches betriebs- und/oder personenbezogene Daten enthält, muss durch Zerreißen des Dokuments und Entsorgung in die eigens dafür vorgesehenen Behälter erfolgen.

I documenti e atti contenenti dati personali sensibili o giudiziari, dovranno essere custoditi in archivi chiusi a chiave.

L'eliminazione fisica di ogni documento cartaceo contenente dati e informazioni aziendali e/o personali deve essere effettuata strappando il documento in più parti e riponendolo negli appositi contenitori.

Art. 6 – Verwaltung betriebs- und personenbezogener Daten

Das gesamte Personal sowie Dritte, welche mit der IDM zusammenarbeiten, ergreifen alle erforderlichen Maßnahmen, um personenbezogene und unternehmensbezogene Daten, betriebliche Prozesse, Knowhow usw., welche sie in Zusammenhang mit Ausübung ihrer Tätigkeit innerhalb der IDM in Erfahrung bringen, geheim zu halten.

Das gesamte Personal sowie Dritte, welche mit der IDM zusammenarbeiten, garantieren zudem alle Daten – archivierte Daten, bearbeitete Daten, in Zusammenhang mit der Ausführung der Tätigkeit erhaltene Dokumente und Informationen - mit strikter Vertraulichkeit zu behandeln und zu schützen.

Jegliche Art der Verarbeitung von Daten und Informationen, welche nicht vom eigenen Verantwortlichen der Datenverarbeitung genehmigt und mit demselben abgesprochen wurde (Übermittlung, Änderung, Kopieren, Löschen, Vermittlung an Außenstehende, Audioaufnahmen und Fotos, usw.), ist untersagt.

Es ist untersagt, betriebsbezogene Daten und Informationen ohne die Erlaubnis und vorherige Absprache mit dem jeweiligen Verantwortlichen der Datenverarbeitung im Internet zu veröffentlichen (soziale Medien, Foren, Chat, Blogs, Websites).

Es ist untersagt, Daten und Informationen in Cloud-Systemen (z.B. Dropbox, Google+, Evernote, usw.) zu speichern, welche vom Systemverwalter nicht autorisiert wurden. Die Cloud-Systeme, in denen Informationen gespeichert werden dürfen, werden von der Direktion in Zusammenarbeit mit dem Systemverwalter festgelegt.

Art. 6 – Gestione dei dati personali e aziendali

Tutto il personale dipendente e tutti i soggetti terzi, che collaborano con IDM si impegnano a mantenere segreto il contenuto di tutti i dati personali e aziendali, informazioni, procedure organizzative, know how di IDM, e di quant'altro vengano a conoscenza nell'ambito dell'esercizio della propria attività lavorativa.

Tutto il personale dipendente e tutti i soggetti terzi, che collaborano con IDM garantiscono altresì la massima riservatezza e protezione dei dati contenuti negli archivi, dei dati elaborati e dei documenti ed informazioni ricevuti nell'ambito dell'esercizio della propria attività lavorativa.

È vietata ogni attività di trattamento di dati e informazioni in qualunque formato (comunicazione, modifica, copia, cancellazione, fornitura ad esterni, video, audio e foto, ecc.) non autorizzata e concordata con il proprio Responsabile del Trattamento.

E' vietato pubblicare in internet (Social media, forum, chat, blog, siti internet) dati ed informazioni di carattere aziendale non autorizzate e concordate con il proprio Responsabile del Trattamento.

È vietato il salvataggio di dati e informazioni in sistemi cloud (per esempio Dropbox, Google+, Evernote, ecc.) non autorizzati dall'Amministratore di sistema. Sarà la Direzione in collaborazione con l'Amministratore di sistema ad indicare i sistemi cloud di salvataggio delle informazioni.

Art. 7 – Zugang zu den Arbeitsmitteln

PC-/Laptop-Arbeitsplatz: Der Gebrauch des PCs und der damit einhergehende Zugang zu Daten, Programmen und EDV-Ressourcen ist im Rahmen der Funktion des Mitarbeiters und der ihm aufgetragenen Aufgaben erlaubt.

Sämtliche PCs sind manuell zu sperren, wenn sie unbewacht gelassen werden und sind zusätzlich mit einem Bildschirmschoner auszustatten, der automatisch nach höchstens 10 Minuten Inaktivität aktiviert wird.

Zugangsdaten und Passwörter: Der Zugang zu den EDV-Systemen erfolgt ausschließlich nach der Identifikation und Authentifizierung des Benutzers mittels Eingabe der Zugangsdaten. Jegliche Änderung der Zugangsdaten zu den Anwendungen, Datenbanken, Archiven, Ordnern und/oder Computerressourcen muss mit dem Verantwortlichen der Datenverarbeitung abgesprochen und von demselben genehmigt werden.

Jeder IDM-Mitarbeiter muss folgende Regeln im Umgang mit dem Passwort befolgen:

- Nur Passwörter verwenden, welche die Komplexitätsanforderungen erfüllen (mindestens 8 alphanumerische Zeichen);
- das Passwort, wie vom System vorgeschrieben, alle 3 Monate ändern;
- das Passwort nicht notieren und im Büro oder online aufbewahren;
- das Passwort nicht in Fragebögen und/oder Formularen angeben;
- die Direktion oder den Systemverwalter kontaktieren, falls jemand versucht, das Passwort zu erfahren;
- darauf achten, das Passwort nicht im Beisein anderer Personen einzugeben, die die Eingabe beobachten könnten;
- nicht die Funktion „Passwort merken“ verwenden, welche in einigen Programmen integriert ist;

Art. 7 – Accesso logico agli strumenti di trattamento

Postazione PC/Notebook: L’utilizzo del PC e conseguentemente l’accesso ai dati, programmi e risorse informatiche, è consentito nei limiti della propria funzione e dei propri incarichi assegnati.

Tutti i PC devono essere bloccati manualmente se lasciati incustoditi e devono essere dotati di uno screen saver, protetto da password, ad attivazione automatica al massimo dopo 10 minuti di inattività.

Credenziali di accesso e password: L’accesso ai sistemi informatici può avvenire esclusivamente previa identificazione a autentica, attraverso la verifica delle proprie credenziali. Qualunque variazione delle abilitazioni di accesso alle applicazioni, banche dati, archivi, cartelle e/o risorse di sistema deve essere concordata ed autorizzata dal Responsabile del Trattamento.

Ogni collaboratore IDM dovrà seguire in particolare la seguente policy per la gestione delle password:

- utilizzare solamente password che rispettino i criteri di complessità previsti (almeno 8 caratteri alfanumerici);
- effettuare un cambio della password ogni 3 mesi, come indicato dal sistema;
- evitare di annotare la propria password all’interno dell’ufficio o di conservarla online;
- evitare di comunicare la propria password su questionari e/o moduli;
- nel caso qualcuno insista nel cercare di conoscere la propria password contattare la Direzione e l’Amministratore di sistema;
- fare attenzione a non digitare la propria password in presenza di altre persone, che potrebbero osservare tale operazione;
- evitare di utilizzare l’opzione “ricorda password” presente in alcuni programmi;

- im Falle des Verlusts und/oder der Zurücksetzung des Passworts muss dem Systemverwalter eine entsprechende Anfrage gesendet werden.

Dritte müssen bei der Verwendung, beim Umgang und bei der Bewahrung der Zugangsdaten zu den Systemen der IDM, welche ihnen vom beauftragten Personal zugewiesen wurden, höchste Vorsicht walten lassen.

Im Bereich der Verwaltung der Zugangsdaten und Benutzerprofile ist es Aufgabe des Systemverwalters, die Zugänge der Benutzer zu überprüfen, und zwar im Falle von:

- Neuinstallationen und Verbesserungen des Computersystems;
- Anomalien oder mangelhafter Funktion des Systems;
- Mitteilungen einzelner Benutzer über eine mangelhafte Funktion des Systems;
- widerrechtlichen Handlungen, die dem Vermögen und/oder dem Ansehen des Unternehmens schaden.

Art. 8 – Software und Download

Die Mitarbeiter der IDM dürfen ausschließlich die der Organisation zur Verfügung stehende Software verwenden.

Soll eine andere als die von der Organisation zur Verfügung gestellte Software getestet oder verwendet werden, ist dazu beim Verantwortlichen für die Datenverarbeitung und dem Systemadministrator eine entsprechende Genehmigung einzuholen.

Jeder Mitarbeiter muss:

- Installationen von Software und/oder Anwendungen vermeiden, welche nicht Eigentum der Organisation sind;
- systematisch sämtliche von außen kommende Dateien überprüfen und angemessene Vorsicht bei der Übermittlung von Dateien nach außen walten lassen;

- Inoltrare una richiesta all'Amministratore di sistema in caso di dimenticanza e/o ripristino della password.

I terzi che collaborano con IDM devono prestare la massima attenzione nell'utilizzo, nella gestione e nella conservazione delle credenziali di autenticazione relative ai sistemi di IDM, assegnate da personale incaricato alla gestione delle utenze.

Nell'ambito della gestione delle credenziali di autenticazione e dei profili utente è compito dell'Amministratore di sistema verificare gli accessi effettuati dagli utenti, nel caso di:

- nuove installazioni e miglioramenti del sistema informatico;
- anomalie e malfunzionamenti del sistema informatico;
- malfunzionamenti segnalati dal singolo utente;
- riscontro di fatti illeciti lesivi del patrimonio e/o dell'immagine aziendale.

Art. 8 – Software e download

Ogni dipendente IDM deve utilizzare esclusivamente i software di cui dispone l'organizzazione, le cui specifiche tecniche sono fornite dall'Amministratore di Sistema.

Qualora sia necessario testare/utilizzare un programma informatico diverso da quelli messi a disposizione dall'organizzazione, è obbligo chiedere l'autorizzazione al Responsabile del trattamento e all'Amministratore di sistema.

Ogni collaboratore deve:

- evitare di installare software e/o applicativi che non appartengano all'organizzazione;
- controllare metodicamente tutti i file provenienti dall'esterno e adottare le opportune cautele al momento della trasmissione all'esterno di file;

- jeglichen Gebrauch von privater Hard- und Software zu Betriebszwecken vermeiden, es sei denn, der Verantwortliche der Datenverarbeitung erteilt eine ausdrückliche Befugnis auf eine schriftliche Anfrage hin (gilt auch für Demoversionen von Software).

Art. 9 – Antivirus-Software

Für den Umgang (Installation, Update usw.) mit der Antivirus-Software ist die IT-Abteilung zuständig. Nichtsdestotrotz ist es notwendig, dass jeder Benutzer:

- das Antivirus-System nicht löscht, aus welchen Gründen auch immer;
- nicht andere als die bereits vom Systemverwalter installierte Antivirus-Software installiert.

Art. 10 – E-Mail

Die Benutzung des zugewiesenen E-Mail-Eingangs darf ausschließlich zu Arbeitszwecken erfolgen. Die Benutzer der E-Mail-Eingänge sind für eine korrekte Verwendung derselben verantwortlich.

Im Besonderen sind folgende Anweisungen zu befolgen:

- Der E-Mail-Eingang des Betriebes darf nicht für das Versenden oder den Erhalt persönlicher Nachrichten verwendet werden;
- der E-Mail-Eingang darf nicht für die Teilnahme an Diskussionen, Foren oder Mailing-Lists verwendet werden, außer wenn von der Direktion ausdrücklich erlaubt;
- für den Fall, dass der Gebrauch des E-Mail-Einganges des Betriebs zu persönlichen Zwecken unbedingt notwendig ist, müssen die Benutzer die Nachrichten persönlicher Natur sofort nach ihrem Versenden/Erhalt löschen;
- geheime, vertrauliche oder im Besitz der IDM befindliche Informationen dürfen, ohne ausdrückliche Genehmigung der Direktion, nicht an Dritte weitergegeben werden;

- evitare qualunque utilizzo di software o applicativi privati per usi aziendali, salvo esplicita autorizzazione da parte del Responsabile del Trattamento previa richiesta scritta (anche per software in versione demo).

Art. 9 – Software Antivirus

La gestione (installazione, aggiornamento, ecc.) del software antivirus è di competenza del Reparto IT. Tuttavia è necessario che ogni utente:

- eviti di disabilitare, per qualsiasi motivo, il sistema antivirus;
- non installi software antivirus diverso da quello già installato dall'Amministratore di sistema.

Art. 10 – Posta elettronica

La casella email assegnata deve essere utilizzata esclusivamente per finalità legate all'attività lavorativa. Gli utenti di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

In particolare devono essere seguite le seguenti disposizioni:

- la casella di posta elettronica aziendale non deve essere utilizzata per l'invio o la ricezione di messaggi personali;
- La casella di posta elettronica aziendale non deve essere utilizzata per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione della Direzione;
- nell'eventualità in cui l'uso personale della posta elettronica aziendale si rendesse eccezionalmente necessario, gli utenti dovranno cancellare i messaggi di natura personale dal sistema non appena trasmessi e/o letti;
- informazioni riservate, confidenziali o comunque di proprietà di IDM non possono essere divulgate a terzi, senza espressa autorizzazione della Direzione;

- es dürfen keine E-Mails oder allgemein Daten, Programme oder sonstiges elektronisches Material mit beleidigendem, verletzendem, vulgärem, gotteslästerlichem, fremdenfeindlichem, pornographischem oder auf eine andere Weise unangebrachtem oder illegalem Inhalt versendet oder aufbewahrt werden;
- im Falle längerer Abwesenheit (Ferien, Krankenstand, Sonderurlaub, längere Tätigkeit außerhalb des Betriebes) muss der Benutzer angemessene Vorbereitungen treffen, um die Kontinuität der Arbeitsvorgänge zu gewährleisten.
- bei Beendigung des Arbeitsverhältnisses (Kündigung) wird der E-Mail-Account des Mitarbeiters durch den Systemadministrator am Werktag nach dem letzten Arbeitstag gelöscht und eine automatische Nachricht eingerichtet, die darauf hinweist, dass der Account nicht mehr verfügbar ist, wobei auf eine andere Geschäfts-E-Mail verwiesen.

Es wird darauf hingewiesen, dass:

- sämtliche eingehende E-Mails von einer Antispam-Software überprüft werden. Trotzdem ist es möglich, dass einige Spam-Mails die Filter des Zentralsystems umgehen: Daher ist es notwendig, höchste Vorsicht im Umgang mit unsicheren Emails walten zu lassen und den Systemverwalter im Falle von zweifelhafter Herkunft/Inhalt derselben darauf hinzuweisen;
- sämtliche eingegangene, gesendete oder gespeicherte Nachrichten von dem Verantwortlichen der Datenverarbeitung und dem Systemverwalter ausschließlich aus folgenden Gründen gelesen werden dürfen:
    - Abwesenheit des Benutzers, um einen regulären Arbeitsablauf zu gewährleisten;
    - Meldungen einzelner Benutzer über eine mangelhafte Funktion des Systems;

- non possono essere inviati ne conservati messaggi di posta elettronica o più in generale dati, programmi o altro materiale di natura informatica dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale;
- in caso di assenza prolungata (ferie, malattia, aspettativa, lunga attività fuori sede) l'utente deve prevedere delle opportune procedure in grado di garantire la continuità delle attività.
- in caso di chiusura del rapporto di lavoro (licenziamento o dimissione), l'email del dipendete sarà disattivata dall'Amministratore di sistema il giorno successivo all'ultimo giorno lavorativo e predisposto un avviso automatico per eventuali terzi (mittenti) di chiusura dell'indirizzo email, segnalando un account aziendale alternativo.

Si avvisa che:

- tutta la posta elettronica in entrata è controllata da un software antispam. È comunque possibile che alcune mail di spam superino i filtri impostati sul sistema centrale: è quindi necessario prestare la massima attenzione a email sospette, avvisando l'Amministratore di sistema in caso di dubbi sulla provenienza/contenuto delle stesse;
- tutti i messaggi ricevuti, spediti o salvati, potranno essere letti dal Responsabile del Trattamento e dall'Amministratore di Sistema esclusivamente per i seguenti motivi:
    - in caso di assenza per garantire una regolare continuità dell'attività lavorativa;
    - in caso di segnalazioni di malfunzionamenti da parte del singolo utente;

- bei widerrechtlichen Handlungen, die dem Vermögen und/oder dem Ansehen des Unternehmens schaden.

In all diesen Fällen wird der Beschäftigte benachrichtigt.

Die **zertifizierte E-Mail (PEC)** kann zum Empfangen und Senden von Nachrichten nur nach vorheriger Ermächtigung durch den Verantwortlichen der Datenverarbeitung verwendet werden.

Art. 11 – Digitale Unterschrift

Die digitale Unterschrift darf nur von Personen verwendet werden, die im Voraus von der Direktion eine entsprechende Genehmigung erhalten haben.

Art. 12 – Navigation im Internet

Der Internetzugang (mittels PC, Tablet oder Betriebssmartphones) dient nur zur die Ausübung der Arbeitstätigkeit. Die Benutzer sind für einen korrekten Umgang mit demselben verantwortlich.

Die Anzahl, Dauer und der Inhalt der Internetzugänge wird ständig aufgezeichnet. Die Einsicht in diese Aufzeichnungen kann nur auf anonyme Weise und in Form von aggregierten Daten in den gesetzlich festgelegten Fällen und bei Missachtung dieser Bestimmungen erfolgen. Etwaige Kontrollen durch den Systemadministrator können durch Analyse der Inhalte oder der Logfile über das Surfverhalten erfolgen.

Zur Vermeidung einer missbräuchlichen Verwendung des Internets verfügt das System über einen Zugangsfilter.

Bei der Benutzung des Internets müssen folgende Regeln beachtet werden:

- Es ist verboten, Material und Programme herunterzuladen, welche urheberrechtlich oder patentrechtlich geschützt sind oder geistiges Eigentum von Personen oder Betrieben sind bzw. Software zu installieren, für welche der Betrieb keine Lizenz besitzt.

- in caso di fatti illeciti lesivi al patrimonio e/o immagine dell'organizzazione.

Il dipendente verrà informato in tutti questi casi.

La **Posta Elettronica Certificata (PEC)** potrà essere utilizzata in lettura e/o scrittura solamente su incarico del Responsabile del Trattamento.

Art. 11 – Firma digitale

La Firma Digitale aziendale potrà essere utilizzata esclusivamente da coloro che sono stati preventivamente autorizzati dalla Direzione.

Art. 12 – Navigazione internet

L'accesso ad Internet (tramite PC, tablet o smartphone aziendali) è fornito per esclusive finalità lavorative. Gli utenti sono responsabili del suo corretto utilizzo.

Il numero, la durata ed il contenuto degli accessi ad Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente Regolamento. Gli eventuali controlli, compiuti dall' Amministratore del sistema, potranno avvenire mediante un sistema di analisi dei contenuti o mediante "file di log" della navigazione svolta.

Per prevenire eventuali abusi nell'uso di Internet il sistema è provvisto di filtri d'accesso.

Si devono osservare le seguenti regole di navigazione:

- È vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno dell'azienda;

- es ist verboten, auf Internetseiten mit unsicherem oder illegalem Inhalt zu navigieren und dort Material herunterzuladen;
- es ist verboten, ohne Genehmigung urheberrechtlich geschütztes Material zu vervielfältigen, etwa durch Digitalisierung und Verbreitung von Fotos aus Magazinen, Büchern oder anderen Quellen, Musik oder Videomaterial;
- es ist verboten, Dateien über eine Peer-to-Peer Verbindung zu teilen;
- es ist verboten, Programme herunterzuladen, auch wenn für diese keine Lizenz benötigt wird oder es sich um Probeversionen handelt (Freeware und Shareware);
- es ist verboten, im Netz oder auf den Servern unerlaubte oder für das System schädliche Software zu verbreiten;
- es ist verboten, die technologische Infrastruktur des Betriebs zu verwenden, um sich gesetzeswidriges Material zu beschaffen und es zu verbreiten;
- es ist verboten, im Internet Tätigkeiten auszuüben, die Sicherheitsprobleme verursachen oder die Kommunikation im Netz stören können;
- jede Form von Überwachung im Netz, durch welche Daten abgefangen werden können, die nicht ausdrücklich dem Host des Benutzers gesendet wurden (Sniffing), ist verboten, sofern dies nicht zu den Aufgaben des Benutzers gehört und somit formell von der Direktion genehmigt ist;
- es ist verboten, den Identifikationsvorgang oder die Sicherheit eines jeden Hosts, Netzes oder Accounts zu umgehen.

Art. 13 – Gebrauch von Smartphones, Betriebstelefonen und Speichermedien

Der Gebrauch des **Telefonnetzes des Betriebs** hat ausschließlich zu Arbeitszwecken zu erfolgen. Um einem unrechtmäßigen Gebrauch des Telefonnetzes vorzubeugen, ist die Überwachung des gesamten Telefonverkehrs vorgesehen.

- è vietato navigare su siti e scaricare materiali pericolosi o aventi contenuti illegali;
- è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso, ma non limitato a, digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- è vietata la condivisione di file in modalità peer-to-peer;
- è vietato scaricare programmi, anche se privi di licenza o in prova (freeware e shareware);
- è vietato immettere sulla rete o sui server software dannosi per i sistemi o comunque non autorizzati;
- è vietato utilizzare l'infrastruttura tecnologica aziendale per procurarsi e diffondere materiale in violazione con le normative vigenti;
- è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;
- è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'utente (sniffing) a meno che questa attività non faccia parte dei compiti dell'utente e quindi formalmente autorizzata dalla Direzione;
- è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

Art. 13 – Utilizzo di smartphone, telefoni aziendali e supporti di memorizzazione

Telefono fisso aziendale: L'utilizzo del telefono aziendale deve essere funzionale esclusivamente allo svolgimento dell'attività lavorativa. Per prevenire eventuali abusi all'uso del telefono è previsto un monitoraggio sul traffico di ogni utenza.

Smartphone und Tablet: Der Zugang zum Smartphone oder Tablet muss mittels Aktivierung eines persönlichen Kennworts (Aktivierung eines automatischen Bildschoners) erfolgen.

Es ist verboten Dokumente, welche als Anlagen heruntergeladen wurden (E-Mail, Skype, usw.) und deren Inhalt mit dem Betrieb zusammenhängt, aufzubewahren, wenn diese nicht mehr benötigt werden.

Beim Gebrauch von Apps muss auf einen angemessenen Datenverbrauch und auf die Sicherheit des Gerätes geachtet werden. Um einem unrechtmäßigen Gebrauch des Telefonnetzes vorzubeugen, ist die Überwachung des gesamten Telefonverkehrs jedes Gerätes vorgesehen.

Bei Entwendung oder Verlust von Smartphones und/oder Tablets hat der Benutzer umgehend den Verantwortlichen der Datenverwaltung und den Systemadministrator zu verständigen, um die Geräte sofort sperren zu lassen und das Verfahren zur Anzeige an die zuständige Behörde einzuleiten.

Nach dem Gebrauch von **Speichermedien** (USB-Sticks, interne und externe Hard Disks, DVDs, CD-ROMs) müssen sämtliche darauf enthaltenen Informationen gelöscht werden.

Art. 14 – VPN

Der Fernzugang zum Unternehmensnetzwerk mittels VPN wird durch den Verantwortlichen der Datenverarbeitung auf Anfrage des Systemadministrators für Arbeitszwecke mit den Modalitäten genehmigt, die vom Unternehmen festgelegt wurden. Aus Sicherheitsgründen werden sämtliche VPN-Zugänge der Benutzer systemseitig aufgezeichnet.

Art. 15 – Überwachungssysteme

Der Systemadministrator hat gemäß den Privacy-Bestimmungen und aus Gründen der Sicherheit des Informationssystems, aus technischen Gründen bzw. zu Wartungszwecken (Updates, Austausch, Einrichtung von Programmen, Wartung von Hardware) bzw. zur Kontrolle und Planung von Betriebskosten (Kosten für Internet, Telefonspesen, usw.) Zugang zu allen Informationssystemen des Unternehmens und allen darin enthaltenen Dokumenten, Anruflisten und Logdateien der Drucker.

Smartphone e Tablet: L'accesso allo Smartphone o Tablet deve avvenire attraverso l'attivazione di una password personale (attivazione dello screen saver automatico).

E' vietata la conservazione di documenti scaricati come allegati (email, Skype, ecc.), il cui contenuto sia di carattere aziendale, se non per il tempo strettamente necessario.

Deve essere posta la massima attenzione all'utilizzo di App sul proprio dispositivo, in relazione all'eccessivo consumo di traffico dati ed alla sicurezza del proprio apparecchio. Per prevenire eventuali abusi è previsto un monitoraggio sulla quantità totale del traffico di ogni utenza.

In caso di furto o smarrimento di Smartphone e/o di Tablet è l'obbligo dell'utente avvisare tempestivamente il Responsabile del trattamento e l'Amministratore di Sistema per permettere il blocco immediato del dispositivo e avviare le procedure di denuncia agli organi competenti.

Al termine dell'utilizzo dei **supporti di memorizzazione** contenenti dati aziendali (chiavette USB, Hard Disk interni ed esterni, DVD, CD-Rom), questi dovranno essere cancellati secondo procedura..

Art. 14 – VPN

Il collegamento alla rete aziendale da remoto attraverso VPN è autorizzato dal Responsabile del trattamento con richiesta all'Amministratore di sistema, per esigenze di lavoro e nelle modalità previste dall'azienda. Per motivi di sicurezza tutti gli accessi realizzati dagli utenti da remoto attraverso VPN sono registrati.

Art. 15 – Sistemi di monitoraggio

È facoltà dell'Amministratore di sistema accedere direttamente a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico e ai servizi di stampa, per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, etc.) nonché per finalità di controllo e programmazione dei costi aziendali (verifica dei costi di connessione ad internet, traffico telefonico, etc.).

Der Systemadministrator hat regelmäßig und bei Auftreten von Störungen (Virusbekämpfung, Verlangsamung der PCs, übermäßige Benutzung des Internets, übermäßiger Speicherplatz des E-Mail-Accounts oder auf der Festplatte usw.) das System einer gründlichen Systemprüfung zu unterziehen, und verschickt, wenn erforderlich, Mitteilungen über die festgestellten Anomalien an die entsprechenden Mitarbeiter.

Individuelle Kontrollen können nur bei wiederholtem Auftreten von Störungen durchgeführt werden.

Art. 16 – Haftung bei Verletzung von Pflichten des Kodex

Die Verletzung von Pflichten vorliegender Bestimmungen gilt als Verhalten gegen die Dienstpflichten und ist ein Disziplinarhaftungsgrund. Aufrecht bleiben sämtliche Fälle, in denen Pflichtverletzungen auch eine strafrechtliche, zivilrechtliche, verwaltungsrechtliche oder buchhalterische Haftung öffentlicher Bediensteter begründen.

Art. 17 – Aktualisierung

Vorliegende Bestimmungen werden regelmäßig aktualisiert. Die jeweils geltende aktuelle Version wird im Intranet des Unternehmens veröffentlicht.

Art. 18 – Zusatzvorschrift

Bei Zweifeln und Unsicherheiten bezüglich der korrekten Verarbeitung personen- und betriebsbezogener Daten und Informationen sowie der Art und Weise des Umgangs mit den Arbeitsmitteln kann sich der Beschäftigte Anleitungen an der Verantwortlicher der Datenverarbeitung wenden.

Periodicamente e in presenza di anomalie (intervento antivirus, segnalazione di rallentamenti del computer, utilizzo aziendalmente eccessivo dell'accesso Internet, dimensione elevata della casella di posta elettronica o dello spazio disco utilizzato, etc.), l'Amministratore di sistema effettuerà verifiche di funzionalità approfondite, inviando, se necessario, segnalazioni a tutti i dipendenti IDM in merito alle anomalie riscontrate.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

Art. 16 – Responsabilità conseguente alla violazione dei doveri del codice

La violazione degli obblighi previsti dal presente Regolamento costituisce comportamento contrario ai doveri d'ufficio ed è fonte di responsabilità disciplinare, ferme restando le ipotesi in cui la violazione possa dar luogo anche a responsabilità penale, civile, amministrativa o contabile del pubblico dipendente.

Art. 17 – Aggiornamento

Il presente Regolamento è soggetto a revisione con frequenza periodica. La versione aggiornata verrà pubblicata sul sito intranet aziendale.

Art. 18 – Prescrizione residuale

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, il dipendente può rivolgersi al Responsabile del Trattamento per ricevere le opportune istruzioni.