

# Documento Programmatico sulla Sicurezza di Arcobaleni196 srl

ai sensi del Codice in materia di protezione dei dati personali art. 34  
e Allegato B, regola 19, del d.lg. 30 giugno 2003, n. 196  
Predisposto il 15 marzo 2008

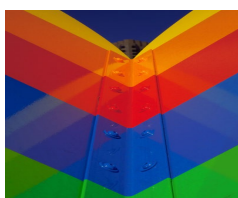


Foto tratta da: [http://commons.wikimedia.org/wiki/Image:Rainbow\\_of\\_hearts.jpg](http://commons.wikimedia.org/wiki/Image:Rainbow_of_hearts.jpg)  
(Photo "Rainbow of Hearts" by Seng P. Merrill; {{Cc-by-sa-2.5|Attribution required:Photo by Seng P. Merrill.}})



Creative Commons Attribuzione-Non commerciale-Non opere derivate 2.5 Italia License

<http://creativecommons.org/licenses/by-nc-nd/2.5/it/>



## Attribuzione-Non commerciale - Non opere derivate 2.5 Italia

<http://creativecommons.org/licenses/by-nc-nd/2.5/it/>

### Tu sei libero:



di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera

### Alle seguenti condizioni:



- **Attribuzione.** Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza e in modo tale da non suggerire che essi avallino te o il modo in cui tu usi l'opera.



- **Non commerciale.** Non puoi usare quest'opera per fini commerciali.



- **Non opere derivate.** Non puoi alterare o trasformare quest'opera, ne' usarla per crearne un'altra.

- Ogni volta che usi o distribuisi quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza.
- In ogni caso, puoi concordare col titolare dei diritti utilizzi di quest'opera non consentiti da questa licenza.
- Questa licenza lascia impregiudicati i diritti morali.

## Indice generale

Introduzione.....	4
Guida alla lettura.....	4
La società.....	5
Struttura organizzativa.....	5
Funzioni organizzative relative alla privacy e protezione dei dati personali.....	6
Responsabile interno per il trattamento dei dati personali.....	6
Responsabili esterni.....	6
Incaricati del trattamento dei dati.....	6
Sistemi informativi.....	7
Elenco dei trattamenti di dati personali (regola 19.1).....	8
Distribuzione dei compiti e delle responsabilità (regola 19.2).....	9
Analisi dei rischi che incombono sui dati (regola 19.3).....	11
Misure in essere (regola 19.4).....	12
Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5).....	13
Pianificazione degli interventi formativi previsti (regola 19.6).....	13
Trattamenti affidati all'esterno (regola 19.7).....	14
Cifratura dei dati o separazione dei dati identificativi (regola 19.8).....	15
Allegati.....	16
Informativa e consenso.....	16
Informativa e consenso al trattamento dei dati personali al sensi del d. lgs. 196/2003 “Codice in materia di protezione dei dati personali” (per i dipendenti).....	16
Informativa al trattamento dei dati personali al sensi del d. lgs. 196/2003 “Codice in materia di protezione dei dati personali” (per i clienti e fornitori).....	17
Nomina a Responsabile.....	18
Nomina a Responsabile (interno) dei trattamenti.....	18
Nomina a Responsabile esterno dei trattamenti.....	18
Elenco incaricati.....	19
Istruzioni per il trattamento dei dati personali.....	20
Informazioni sull'autore di questo documento.....	21

## Introduzione

Il presente Documento Programmatico sulla Sicurezza (DPS) è stato redatto nel **marzo 2008** da **Arcobaleni196 srl** sulla base delle indicazioni contenute nella “Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)”<sup>1</sup> e nella “Guida pratica e misure di semplificazione per le piccole e medie imprese”<sup>2</sup> predisposte dal Garante per la Protezione dei dati personali.

Il DPS è stato predisposto da un gruppo di lavoro aziendale composto da :

- Arcobaleni Pino – Direttore Generale e “Responsabile per il trattamento dei dati personali”,
- Rossetti Carmela – Responsabile Qualità e Controlli,
- Marroni Ercole – Responsabile Produzione, con l'ausilio di:
  - White Pino – Sistemi e Reti,
- Nerucci Giuseppina – Gestione Risorse Umane,
- Nerini Mariuccia – Contabilità.

Copia del presente documento, compresi gli allegati, è disponibile presso il “Responsabile per il trattamento dei dati personali” che ne cura gli aggiornamenti.

## Guida alla lettura

Il DPS è articolato in capitoli seguendo il modello proposto dal Garante. Ogni capitolo si riferisce ad uno dei punti indicati come obbligatori alla regola 19 dell'allegato B, “Disciplinare tecnico in materia di misure minime di sicurezza”<sup>3</sup>, al “Codice in materia di protezione dei dati personali”<sup>4</sup> (si noti che il punto 19.8 non è però applicabile in quanto si riferisce alle aziende esercenti professioni sanitarie). Oltre a tali capitoli sono stati inseriti:

- un capitolo preliminare che descrive brevemente la società;
- un capitolo finale che comprende allegati, modulistica e documenti di approfondimento.

---

1 Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS) in <http://www.garanteprivacy.it/garante/document?ID=1007740&DOWNLOAD=true>

2 Guida pratica e misure di semplificazione per le piccole e medie imprese in <http://www.garanteprivacy.it/garante/doc.jsp?ID=1412271>

3 Disciplinare tecnico in materia di misure minime di sicurezza, allegato B al Codice in materia di protezione dei dati personali, in <http://www.garanteprivacy.it/garante/doc.jsp?ID=488497>

4 Codice in materia di protezione dei dati personali in <http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248>

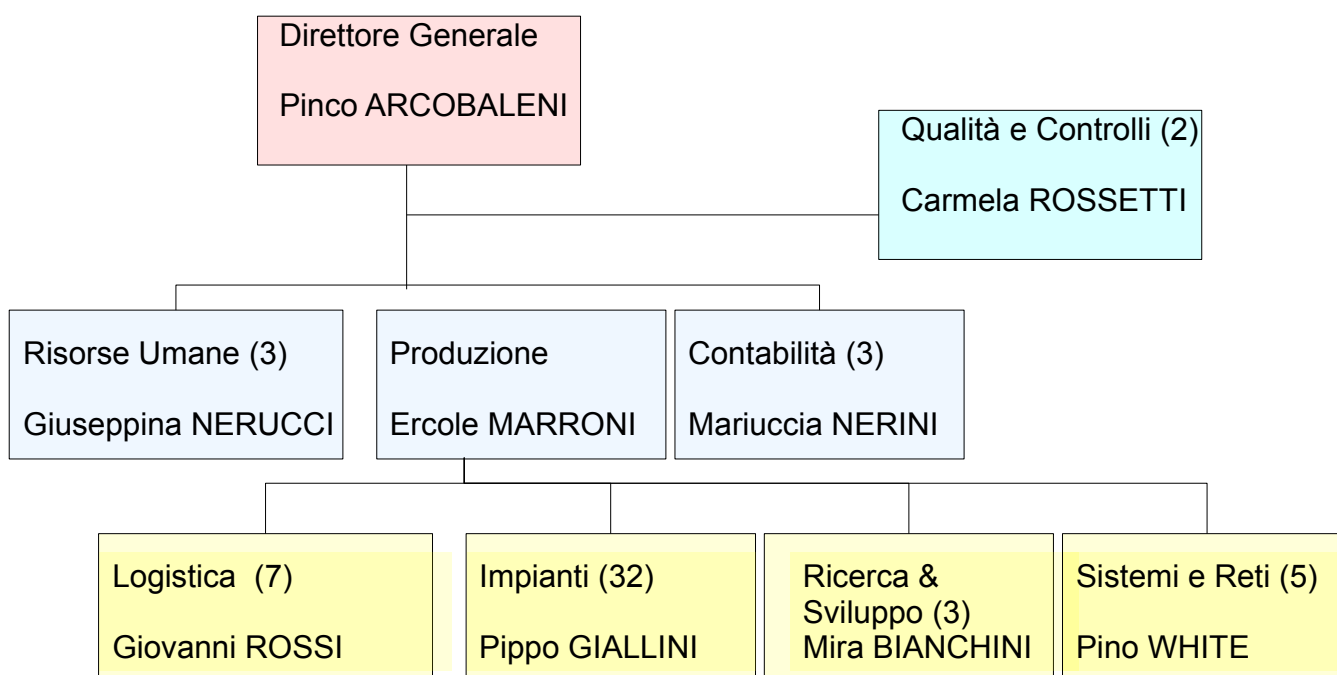
## La società

Arcobaleni196 srl è una società specializzata nella produzione di vernici speciali per la carrozzeria di veicoli. La società, detentrica di numerosi brevetti nazionali ed internazionali, fornisce i suoi prodotti alle principali case automobilistiche mondiali. La sede unica è ubicata presso Colleazzurro nella provincia di Roma. La società è certificata secondo la norma UNI EN ISO 9001:2000 per tutte le proprie attività.

## Struttura organizzativa

Di seguito è riportato l'organigramma della società alla data di redazione del documento.

### Organigramma di Arcobaleni srl 12 febbraio 2008



Alla data i dipendenti sono 57.

## **Funzioni organizzative relative alla privacy e protezione dei dati personali**

### **Responsabile interno per il trattamento dei dati personali**

Il Cda ha nominato, ai sensi dell'articolo 29 del Codice, il Direttore Generale “Responsabile interno” per i trattamenti dei dati personali, dandogli istruzioni operative scritte sulle modalità operative e sulle misure di sicurezza da adottare. Contestualmente alla nomina, il Direttore Generale ha ricevuto dal CdA delega scritta per la nomina dei responsabili esterni del trattamento.

Il “Responsabile interno” avvalendosi dei responsabili delle altre unità operative e, ove necessario, dei consulenti esterni (legale, fiscale, del lavoro):

- redige, aggiorna almeno annualmente, conserva il Documento Programmatico della Sicurezza;
- censisce ed aggiorna l'elenco dei trattamenti dei dati personali in azienda e garantisce il diritto d'accesso come previsto dalle norme sulla privacy;
- con l'assistenza del responsabile “Sistemi e Reti” individua, predispone, verifica, documenta e rende note le misure di sicurezza (minime e più ampie) necessarie per la protezione dei dati personali.

In allegato è riportata **copia della lettera di nomina**.

### **Responsabili esterni**

Il Responsabile dei trattamenti, in virtù della delega ricevuta dal CdA, ha nominato “Responsabili esterni” per i trattamenti dei dati personali, dando istruzioni operative scritte sulle modalità operative e sulle misure di sicurezza da adottare:

- la società **Sicurezza1** per i trattamenti relativi agli adempimenti 626 sulla sicurezza sul posto di lavoro,
- gli studi legali **Avvocati1** e **Avvocati2** per i trattamenti relativi agli adempimenti giuslavoristi, la contrattualistica, gli aspetti legali,
- studio **Fiscalista1** per i trattamenti relativi agli adempimenti fiscali,
- società **Sorveglianza1** per i trattamenti relativi alla guardiania degli edifici,
- società **Pulizia1** per i trattamenti relativi alla pulizia degli edifici,
- società **Software1** e **Software2** per i trattamenti relativi rispettivamente al sistema informativo “amministrativo contabile” e “logistico” entrambi in outsourcing.

In allegato è riportata **copia del modello di lettera di nomina**.

### **Incaricati del trattamento dei dati**

Ciascun dipendente è assegnato stabilmente, all'atto dell'assunzione o nel caso di cambiamento di mansione, presso una o più strutture organizzative presso cui sono trattati i dati e per ciascuna delle

quali sono individuate (vedi capitolo “**Distribuzione dei compiti e delle responsabilità - regola 19.2**”) le categorie di dati cui si può avere accesso e gli ambiti del trattamento. Nella lettera di assunzione sono indicate le istruzioni da seguire nel trattamento dei dati.

Analogamente sono considerati incaricati, mediante incarico sottoscritto dalle parti all'atto della stipula dei contratti, per il solo periodo necessario, anche i consulenti (in proprio o di società terze) nonché gli addetti alla manutenzione SW e HW nei casi in cui la loro attività comporti operazioni di trattamento.

In ogni caso a tutti gli incaricati sono state fornite istruzioni scritte per operare con la massima diligenza ed attenzione in tutte le fasi di trattamento rispettando le misure di sicurezza predisposte dalla società.

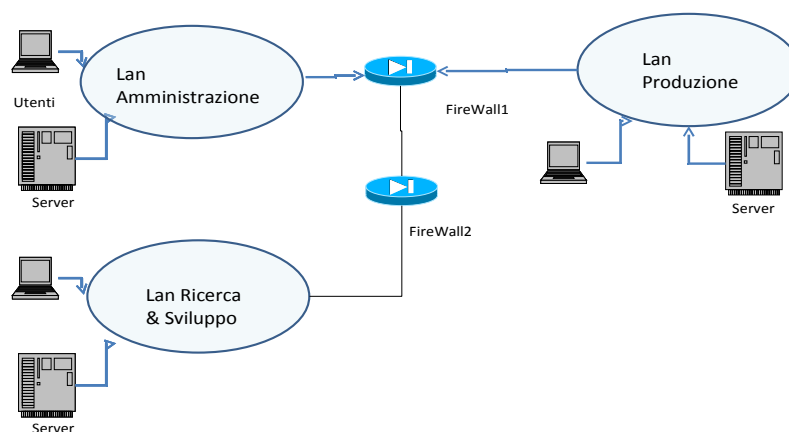
In allegato è riportata l'**elenco degli incarichi** suddivisa per unità organizzativa di competenza e le **istruzioni** per il trattamento dei dati.

## Sistemi informativi

I sistemi informativi di Arcobaleni 196 si basano su tre reti locali (LAN):

1. Lan di amministrazione utilizzata per la Contabilità, la Qualità, le Risorse Umane e la Direzione Generale;
2. Lan di produzione utilizzata esclusivamente per il ciclo produttivo;
3. Lan “ricerca e sviluppo” utilizzata esclusivamente per la prototipazione dei nuovi manufatti.

### Schema sistema informativo



L'accesso ad Internet è controllato mediante un firewall (denominato firewall1) che filtra le comunicazioni secondo le regole decise. Un secondo firewall (denominato firewall2) separa la Lan “ricerca e sviluppo” dalle altre reti aziendali. Tutti i server e client sono dotati di antivirus aggiornati centralmente via Lan almeno giornalmente. Tutti i server sono dotati di gruppi di continuità e sistemi di back-up giornalieri automatici.

## Elenco dei trattamenti di dati personali (regola 19.1)

In questa sezione sono censiti i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
Finalità perseguita o attività svolta	Categorie di interessati					
Paghe e contributi	Personale dipendente	X	X	Risorse Umane	Società Software 1	PC collegati in Lan, Internet
Gestione personale	Personale dipendente	X	X	Risorse Umane	Società Software 1	PC collegati in Lan, Internet
Legge 626 e sicurezza del personale	Personale dipendente	X		Risorse Umane	Società Sicurezza1	Internet, PC stand Alone
Fatturazione attiva	Clienti			Contabilità		PC collegati in Lan, Internet
Acquisti e gestione fornitori	Fornitori			Contabilità		PC collegati in Lan, Internet
Ciclo di produzione	Clienti, fornitori			Produzione	Società Software 2	PC collegati in Lan, Internet
Gestione Qualità	Personale dipendente			Qualità e Controlli		PC collegati in Lan
Adempimenti societari	Personale dipendente	X		Qualità e Controlli	Studi legali 1 e 2	PC collegati in Lan
Guardania, visitatori	Personale dipendente, Visitatori, Clienti, Fornitori			Qualità e Controlli	Società Sorveglianza1	PC collegati in Lan
Prototipi	Clienti, fornitori			Ricerca e Sviluppo		PC Stand Alone

### Legenda

- Descrizione sintetica: definizione del trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es., fornitura di beni o servizi, gestione del personale, ecc.) e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.).
- Natura dei dati trattati: indicazione se, tra i dati personali, sono presenti dati sensibili (S) o giudiziari (G).
- Struttura di riferimento: indica la struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento.



- Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture va indicata, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.
- Descrizione degli strumenti elettronici utilizzati: va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi).

## Distribuzione dei compiti e delle responsabilità (regola 19.2)

In questa sezione sono descritte sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Risorse Umane	Paghe e contributi	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi
Risorse Umane	Gestione personale	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi
Risorse Umane	Legge 626 e sicurezza del personale	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi
Contabilità	Fatturazione attiva	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc)
Contabilità	Acquisti e gestione fornitori	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc)
Produzione	Ciclo di produzione	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc)
Qualità e Controlli	Gestione Qualità	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc)
Qualità e Controlli	Adempimenti societari	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc)
Qualità e Controlli	Guardania, visitatori	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc)
Ricerca e Sviluppo	Prototipi	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc)

Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		S	G			
Finalità perseguita o attività svolta	Categorie di interessati					
Paghe e contributi	Personale dipendente	X	X	Risorse Umane	Società Software 1	PC collegati in Lan, Internet
Gestione personale	Personale dipendente	X	X	Risorse Umane	Società Software 1	PC collegati in Lan, Internet
Legge 626 e sicurezza del personale	Personale dipendente	X		Risorse Umane	Società Sicurezza1	Internet, PC stand Alone
Fatturazione attiva	Clienti			Contabilità		PC collegati in Lan, Internet
Acquisti e gestione fornitori	Fornitori			Contabilità		PC collegati in Lan, Internet
Ciclo di produzione	Clienti, fornitori			Produzione	Società Software 2	PC collegati in Lan, Internet
Gestione Qualità	Personale dipendente			Qualità e Controlli		PC collegati in Lan
Adempimenti societari	Personale dipendente	X		Qualità e Controlli	Studi legali 1 e 2	PC collegati in Lan
Guardania, visitatori	Personale dipendente, Visitatori, Clienti, Fornitori			Qualità e Controlli	Società Sorveglianza1	PC collegati in Lan
Prototipi	Clienti, fornitori			Ricerca e Sviluppo		PC Stand Alone

## Legenda

- Struttura: riporta le indicazioni delle strutture già menzionate nella precedente sezione.
- Trattamenti effettuati dalla struttura: indicare i trattamenti di competenza di ciascuna struttura.
- Compiti e responsabilità della struttura: descrive sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.). Anche in questo caso è possibile utilizzare, nei termini predetti, altri documenti già predisposti.

## Analisi dei rischi che incombono sui dati (regola 19.3)

In questa sezione sono indicati i principali eventi potenzialmente dannosi per la sicurezza dei dati nonché la valutazione delle possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

<b>Rischi</b>	<b>Si/No</b>	<b>Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)</b>
<b>Comportamenti degli operatori</b>		
sottrazione di credenziali di autenticazione	Si	alta
carenza di consapevolezza, disattenzione o incuria	Si	media
comportamenti sleali o fraudolenti	Si	alta
errore materiale	Si	media
altro evento		
<b>Eventi relativi agli strumenti</b>		
azione di virus informatici o di programmi suscettibili di recare danno	Si	alta
spamming o tecniche di sabotaggio	Si	media
malfunzionamento, indisponibilità o degrado degli strumenti	Si	alta
accessi esterni non autorizzati	Si	alta
intercettazione di informazioni in rete	Si	media
altro evento		
<b>Eventi relativi al contesto</b>		
sottrazione di strumenti contenenti dati	Si	media
eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	Si	alta
guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Si	media
errori umani nella gestione della sicurezza fisica	Si	media
altro evento		

### Legenda

- Elenco degli eventi: elenca gli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali.
- Impatto sulla sicurezza: descrive le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento, e valuta la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'evento.

## Misure in essere (regola 19.4)

In questa sezione sono riportate, in forma sintetica, le misure in essere per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Struttura o persone addette all'adozione
Videosorveglianza alla reception, badge per l'ingresso al piano	Ingressi non autorizzati a locali/aree ad accesso ristretto	Tutti	Guardiana, Gestione Risorse Umane
	sottrazione di strumenti contenenti dati		
Piano di Disaster Recovery; back-up dei dati in rete	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria	Tutti	Sistemi e Reti
Formazione	errori umani nella gestione della sicurezza fisica	Tutti	Tutti
Formazione	carenze di consapevolezza;	Tutti	Tutti
Formazione	disattenzione o incuria;	Tutti	Tutti
Controlli automatici e manuali	comportamenti sleali o fraudolenti;	Tutti	Tutti
Antivirus, gestione patch	Azione di virus informatici o di programmi suscettibili di recare danno;	Tutti	Tutti
Antivirus, gestione patch	spamming o tecniche di sabotaggio;	Tutti	Tutti
Firewal	accessi esterni non autorizzati;	Tutti	Tutti
Firewal	accessi esterni non autorizzati;	Tutti	Tutti

### Legenda

- Misure: descrive sinteticamente le misure adottate (seguendo anche le indicazioni contenute nelle altre regole dell'Allegato B del Codice).
- Descrizione dei rischi: per ciascuna misura indica sinteticamente i rischi che si intende contrastare (anche qui, si possono utilizzare le indicazioni fornite dall'Allegato B).
- Trattamenti interessati: indica i trattamenti interessati per ciascuna delle misure adottate. Determinate misure possono non essere riconducibili a specifici trattamenti o banche di dati

(ad esempio, con riferimento alle misure per la protezione delle aree e dei locali).

- Struttura o persone addette all'adozione: indica la struttura o la persona responsabili o preposte all'adozione delle misure indicate.

## **Criteria e modalità di ripristino della disponibilità dei dati (regola 19.5)**

In questa sezione sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati.

### **Ripristino**

<b>Banca /data base/archivio di dati</b>	<b>Criteri e procedure per il salvataggio e il ripristino dei dati</b>	<b>Pianificazione delle prove di ripristino</b>
Trattamenti Lan Amministrazione	Back-up giornaliero su server	Mensili
Produzione	Back-up giornaliero su server	Mensili
Trattamenti Lan Ricerca e Sviluppo	Back-up giornaliero su server	Mensili

### **Legenda**

- Banca dati/Data base/Archivio: indica la banca dati, il data base o l'archivio interessati.
- Criteri e procedure per il salvataggio e il ripristino dei dati: descrive sinteticamente le procedure e i criteri individuati per il salvataggio e il ripristino dei dati.
- Pianificazione delle prove di ripristino: indica i tempi previsti per effettuare i test di efficacia delle procedure di salvataggio/ripristino dei dati adottate.

## **Pianificazione degli interventi formativi previsti (regola 19.6)**

In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Corso base privacy (auto-formazione e online)	Nuovi assunti	Prima di iniziare i trattamenti
Corso privacy per Risorse umane (auto-formazione e online)	Risorse umane	secondo semestre 2008

### Legenda

- Descrizione sintetica degli interventi formativi: sono descritti sinteticamente gli obiettivi e le modalità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 (ingresso in servizio o cambiamento di mansioni degli incaricati, introduzione di nuovi elaboratori, programmi o sistemi informatici, ecc) .
- Classi di incarico o tipologie di incaricati interessati: sono individuati le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati, anche in riferimento alle strutture di appartenenza.
- Tempi previsti: sono indicati i tempi previsti per lo svolgimento degli interventi formativi.

### Trattamenti affidati all'esterno (regola 19.7)

In questa sezione è riportato il quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Outsourcing paghe	Gestione paghe	Società SW1	Nomina a Responsabile
Outsourcing logistica	Gestione produzione	Società SW2	Nomina a Responsabile

### Legenda

- Descrizione dell'attività "esternalizzata": è indicata sinteticamente l'attività affidata all'esterno.

- Trattamenti di dati interessati: è indicato se i trattamenti sono relativi a dati, sensibili o giudiziari, effettuati nell'ambito della predetta attività.
- Soggetto esterno: è indicata la società, l'ente o il consulente cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento).
- Descrizione dei criteri: il tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale:
  1. trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
  2. adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
  3. rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
  4. impegno a relazionare periodicamente sulle misure di sicurezza adottate –anche mediante eventuali questionari e liste di controllo- e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

## **Cifratura dei dati o separazione dei dati identificativi (regola 19.8)**

Non applicabile in quanto questo punto riguarda solo organismi sanitari e esercenti professioni sanitarie (regola 24).

## Allegati

### Informativa e consenso

#### **Informativa e consenso al trattamento dei dati personali al sensi del d. lgs. 196/2003 “Codice in materia di protezione dei dati personali” (per i dipendenti)**

Arcobaleni196, con sede in via Multicolori 123, ColleAzzurro (Roma), effettua trattamenti di Suoi dati personali nel pieno rispetto delle norme di legge secondo principi di correttezza, liceità e trasparenza e per finalità strettamente connesse e strumentali alla gestione del rapporto di lavoro, ivi comprese le finalità previdenziali, e in particolare:

- per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- per eseguire obblighi derivanti dal Suo contratto di lavoro.

Può accadere che per l’adempimento di specifici obblighi relativi alla gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e di previdenza e assistenza, Arcobaleni196 tratti i dati che la legge definisce come sensibili e cioè quelli idonei a rilevare l’origine razziale o 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, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale.

Rispetto al trattamento di tali dati, Le ricordiamo che non è richiesto dalla legge il Suo consenso nel caso di trattamento necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria.

Il Suo consenso al trattamento dei dati sensibili è invece richiesto dalla legge nel caso di trattamento necessario per adempiere ad obblighi previsti da contratti collettivi, anche aziendali (ad esempio, trattenute sindacali, corresponsioni di liberalità o benefici accessori).

Senza il Suo consenso non potranno essere eseguite le conseguenti operazioni.

Il trattamento dei Suoi dati personali avviene mediante strumenti informatici, telematici e manuali, con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza degli stessi e sempre nel rispetto delle previsioni di cui all’art. 11 del D.Lgs. 196 del 2003.

Per lo svolgimento, per nostro conto, di talune delle attività relative al trattamento dei Suoi dati personali, la società effettua comunicazioni a società o enti esterni di fiducia, nostri diretti collaboratori che operano in totale autonomia come distinti “titolari” del trattamento. Si tratta, in modo particolare, di soggetti che svolgono servizi di paghe e contributi, gestione di forme di previdenza e assistenza, erogazioni dei buoni pasto ed altri servizi affini. Il loro elenco è costantemente aggiornato e può conoscerlo agevolmente e gratuitamente chiedendolo al Responsabile del trattamento.

Firmato

Il Responsabile del trattamento



## **Consenso al trattamento dei dati personali**

Spett.le Arcobaleni196 srl

Premesso che – come rappresentato nell’informativa che mi è stata fornita ai sensi del D.Lgs. 30/6/2003 n. 196 – può accadere che il trattamento di taluni dei miei dati sensibili derivi dall’adempimento di obblighi previsti dal contratto collettivo, anche aziendale

- do il consenso
- nego il consenso

Sono consapevole che, in mancanza di consenso, non potranno essere eseguite le conseguenti operazioni.

Data \_\_\_\_\_ Firma \_\_\_\_\_

## **Informativa al trattamento dei dati personali ai sensi del d. lgs. 196/2003 “Codice in materia di protezione dei dati personali” (per i clienti e fornitori)**

Ai sensi dell’art. 13 del d. lgs. 196/2003 “Codice in materia di protezione dei dati personali” ed in relazione al rapporto contrattuale in essere con la nostra azienda, si informa che i Vostri dati personali formeranno oggetto di trattamento, e più precisamente che:

- le finalità del trattamento sono relative all’esecuzione degli obblighi derivanti dal rapporto contrattuale e ad ogni incombenza ad esso strettamente correlata nonché a obblighi derivanti da leggi, regolamenti e normativa comunitaria;
- le modalità del trattamento possono prevedere l’utilizzo di mezzi cartacei e informatici atti a memorizzare e gestire i dati stessi, mediante strumenti idonei a garantire la loro sicurezza e la riservatezza;
- i dati da Voi forniti potranno essere oggetto di comunicazione, nel pieno rispetto delle prescrizioni di legge, per finalità strettamente correlate all’esecuzione dei nostri obblighi contrattuali.
- possono venire a conoscenza dei dati, in qualità di incaricati o responsabili, i dipendenti e i collaboratori esterni addetti alla Funzione Contabilità Fornitori nonché soggetti, interni ed esterni, che svolgono per conto della società compiti tecnici, di supporto (in particolare, servizi legali, servizi informatici, spedizioni) e di controllo aziendale.

Vi ricordiamo che l’art. 7 del D.Lgs. 196 del 2003 Vi riconosce taluni diritti. In particolare Voi potrete:

- ottenere la conferma della esistenza o meno di dati personali che Vi riguardano, e che tali dati Vi vengano comunicati in forma intelligibile;
- ottenere l’indicazione dell’origine dei dati, delle finalità e modalità del trattamento, della logica applicata nel caso di trattamento con l’ausilio di strumenti elettronici, degli estremi identificativi del titolare e del responsabile, dei soggetti o delle categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza;
- ottenere l’aggiornamento, la rettifica o, quando vi avete interesse, l’integrazione dei dati; la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione

di legge; l'attestazione che tali operazioni sono state portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi (quando ciò non si riveli impossibile o sproporzionato rispetto al diritto tutelato);

- opporVi in tutto o in parte, per motivi legittimi, al trattamento dei Vostri dati personali ancorché pertinenti allo scopo della raccolta, o quando siano trattati ai fini di invio di materiale pubblicitario o di vendita diretta o di ricerche di mercato o di comunicazione commerciale.

Per l'esercizio di tali diritti, potrete rivolgerVi al responsabile del trattamento di Arcobaleni196 domiciliato per le funzioni presso la sede legale della società al quale ci si può rivolgere via email [privacy@arcobaleni196](mailto:privacy@arcobaleni196).

## **Nomina a Responsabile**

### **Nomina a Responsabile (interno) dei trattamenti**

*(Delibera del Consiglio di Amministrazione)*

Ai sensi dell'art.29 del decreto legislativo 30 giugno 2003 n. 196 “Codice in materia di trattamento dei dati personali”, il Consiglio delibera la nomina del Direttore Generale della società quale “Responsabile del trattamento dei dati”, concedendo allo stesso la delega a nominare, per conto del Titolare, ulteriori responsabili (anche esterni) di specifici trattamenti.

La nomina avviene dopo aver constatato che il Direttore Generale, in relazione al grado ricoperto in azienda che gli permette di avvalersi della collaborazione di tutte le strutture e le risorse interne, nonché dei poteri di firma e di spesa, possiede i requisiti di esperienza, capacità ed affidabilità idonei a fornire garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento.

Il “Responsabile interno” avvalendosi dei responsabili delle altre unità operative e, ove necessario, dei consulenti esterni (legale, fiscale, del lavoro):

- redige, aggiorna almeno annualmente, conserva il Documento Programmatico della Sicurezza;
- censisce ed aggiorna l'elenco dei trattamenti dei dati personali in azienda e garantisce il diritto d'accesso come previsto dalle norme sulla privacy;
- con l'assistenza del responsabile “Sistemi e Reti” individua, predispone, verifica, documenta e rende note le misure di sicurezza (minime e più ampie) necessarie per la protezione dei dati personali.

### **Nomina a Responsabile esterno dei trattamenti**

Spettabile **Società Software1**

Arcobaleni196 srl, è “Titolare” di trattamenti di dati personali che sono esternalizzati presso la Vs. Azienda, per effetto del contratto stipulato il 21 settembre 2005, rif. ABC1230. Con la presente Arcobaleni196 designa la Vs. Azienda quale “Responsabile del trattamento” ai sensi dell'art. 29 del d. lgs. 196/2003 “Codice in materia di protezione dei dati personali” (il “Codice”) in relazione ai trattamenti previsti nel contratto suddetto.

In relazione a tale nomina la Vs. Azienda dovrà seguire le seguenti istruzioni:

- garantire che i trattamenti siano svolti nel pieno rispetto delle norme e di ogni prescrizione contenuta nel Codice, nei relativi allegati compresi i codici deontologici, delle future modificazioni ed integrazioni nonché informarsi e tenere conto dei provvedimenti, dei comunicati ufficiali, delle autorizzazioni generali emessi dall'Autorità Garante per la Protezione dei Dati Personali (il “Garante”);
- verificare la costante adeguatezza delle misure di sicurezza per la protezione dei trattamenti alle misure minime di sicurezza di cui agli artt. da 33 a 35 del Codice, da adottarsi nei modi previsti dal Disciplinare Tecnico allegato B al Codice e secondo le previsioni dell’art. 180, e delle eventuali modificazioni o integrazioni che dovessero intervenire ai sensi dell’art. 36 nonché a quelle idonee e preventive di cui all’art. 31 così da ridurre al minimo i rischi di perdita e distruzione, anche accidentale, dei dati stessi, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta;
- segnalare tempestivamente qualsiasi eventuale carenza sulle misure di sicurezza adottate o su qualunque altro aspetto relativo ai trattamenti conferiti che dovesse comportare responsabilità civili e penali del Titolare;
- curare l’aggiornamento periodico, almeno annuale, del Documento Programmatico sulla sicurezza previsto dalla regola 19 del Disciplinare Tecnico citato, relativamente ai trattamenti di dati personali conferiti col contratto suddetto, consegnandone copia in tempo utile affinché Arcobaleni196 possa provvedere all’adempimento rispettando la scadenza prevista dalla normativa in questione;
- comunicare tempestivamente qualsiasi richiesta ricevuta ai sensi dell'art. 7 del Codice, per consentirne l'evasione nei termini previsti dalla legge e, in particolare, disporre l'organizzazione interna per l'eventuale modifica, rettifica, integrazione e cancellazione dei dati, nonché il blocco del trattamento ove venisse disposto dal Garante o dall'Autorità Giudiziaria;

Ci riserviamo, ai sensi dell'art. 29 comma 5 del Codice, la facoltà di effettuare verifiche periodiche per vigilare sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, e delle istruzioni suddette.

Cordiali saluti

## Elenco incaricati

(esempio)

Unità Organizzativa	Cognome	Nome
Direzione Generale	Arcobaleni	Pino
Qualità e Controlli	Rossetti	Carmela
Risorse Umane	Nerucci	Giuseppina
Risorse Umane	Bianchi	Walter
Risorse Umane	Rossi	Paolino
Contabilità	Nerini	Mariuccia
Contabilità	Neretti	Aldo

<b>Unità Organizzativa</b>	<b>Cognome</b>	<b>Nome</b>
Contabilità	Nerucci	Erika

## **Istruzioni per il trattamento dei dati personali**

Ai sensi dell'art. 30 d. lgs. 196/2003 “Codice in materia di protezione dei dati personali” (il “Codice”) di seguito Le sono fornite le istruzioni per il trattamento dei dati personali a cui Lei è incaricato.

Nel trattare i dati personali, sia se riferiti a persone fisiche, sia se riferiti a soggetti giuridici e indipendentemente dalla natura ordinaria o particolare dei dati, si deve operare garantendo la massima riservatezza delle informazioni, considerando tutti i dati personali confidenziali e, di norma, soggetti al segreto d'ufficio; fatta eccezione per i soli dati anonimi, generalmente trattati per elaborazioni statistiche, e quelli acquisibili da chiunque perché contenuti in atti, liste ed elenchi pubblici (seguendo comunque le prescrizioni di legge).

La procedura di lavoro e la condotta tenuta nello svolgimento delle operazioni di trattamento, dovranno evitare che i dati personali siano soggetti a rischi di distruzione e perdita anche accidentale; che ai dati possano accedere persone non autorizzate; che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati sono stati raccolti.

Si deve dunque operare con la massima diligenza ed attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, all'eventuale loro aggiornamento, così per la conservazione ed eventuale cancellazione o distruzione.

Non possono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal responsabile diretto, comunque riferiti alle disposizioni e regolamenti vigenti.

I dati personali particolari possono essere trattati esclusivamente dagli incaricati, ivi compresi i diretti superiori degli incaricati stessi, secondo l'appartenenza alle seguenti classi omogenee:

- Direzione Generale
- Qualità e Controlli
- Risorse Umane
- Contabilità
- Produzione
- Ricerca e Sviluppo

## Informazioni sull'autore di questo documento



L'ingegner **Panfilo Marcelli** ha lavorato per oltre vent'anni presso primarie aziende informatiche e di consulenza (IPACRI, Euros Consulting, OASI Servizi) con incarichi, anche direttivi, in ambito Information Technology, Privacy e Protezione dei dati personali, Qualità e Certificazione ISO9000 e ISO27001, Workflow Management e Business Process Reengineering, Internet, Intranet e gestione di siti con sistemi CMS.

Attualmente é socio di CMA Consulting (<http://www.cmaconsulting.it/>) società specializzata in servizi, consulenza e formazione in ambito Compliance, Privacy, Qualità e Sicurezza.

Può essere contattato via email: [p.marcelli@cmaconsulting.it](mailto:p.marcelli@cmaconsulting.it)