



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Valido fino al 31 Marzo 2009.

Documento riassuntivo delle misure di sicurezza per la Privacy attuate dal Titolare, in conformità agli artt. da 33 a 36 ed all'allegato B del D.Lgs. 30 giugno 2003, n. 196.

INDICE DEI DOCUMENTI PRESENTI

Organigramma : elenco dei trattamenti, dei compiti e delle responsabilità della privacy.

Soggetti Autorizzati : elenco del personale autorizzato ad accedere agli archivi dopo l'orario di chiusura.

Analisi dei Rischi : analisi dei rischi, misure adottate e piano di miglioramento.

Ripristino dei dati : piano per il ripristino dei dati in caso di danneggiamento o distruzione.

Piano di Formazione : piano di formazione degli incaricati del trattamento.

Trattamenti Esterni : elenco trattamenti esterni e dei criteri adottati per garantire l'adozione delle misure minime.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

ELENCO DEI TRATTAMENTI E DISTRIBUZIONE DEI COMPITI

Descrizione dei dati personali trattati, suddivisi per banche dati ed unità di archiviazione, ed organigramma della distribuzione dei compiti e delle responsabilità per il trattamento e la gestione dei dati.

La descrizione dettagliata delle aree di competenza, dei compiti e delle istruzioni affidati ai singoli soggetti è reperibile consultando la corrispondente nomina a responsabile od ad incaricato.

Titolare del trattamento : GAIN STUDIOS DI AROSIO ELVIO S.A.S. nella persona di ELVIO AROSIO

Responsabile al rapporto con gli interessati (art. 13) : ELVIO AROSIO

Sedi interessate ai trattamenti dei dati personali.

Sale Prove C/o Scuola Don Minzoni

<i>Indirizzo:</i>	Via Turati , 27100 Pavia (PV)
<i>Responsabili:</i>	<ul style="list-style-type: none"> Responsabile della sicurezza : ELVIO AROSIO Responsabile dei sistemi di elaborazione elettronica : ELVIO AROSIO
Sono sotto riportati gli uffici od i locali della sede interessati al trattamento od alla conservazione dei dati personali.	
<ul style="list-style-type: none"> Sala Attesa 	Sala di attesa con computer per la videosorveglianza

Sede Principale Azienda

<i>Indirizzo:</i>	Sede Principale azienda Viale Montegrappa 28/G , 27100 PAVIA (PV); e-mail: info@gainstudios.com; telefono: 0382 464161
<i>Responsabili:</i>	<ul style="list-style-type: none"> Responsabile della sicurezza : ELVIO AROSIO Responsabile dei sistemi di elaborazione elettronica : ELVIO AROSIO
Sono sotto riportati gli uffici od i locali della sede interessati al trattamento od alla conservazione dei dati personali.	
<ul style="list-style-type: none"> Ufficio Direzionale 	Ufficio al Primo Piano della sede principale

Banche Dati

Banca Dati : Acquisti

Dati anagrafici, Fatture, Ddt, Ordini, Preventivi, Documenti bancari, Rubriche, Corrispondenza

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> Codice fiscale ed altri numeri di identificazione personale Nominativo, indirizzo o altri elementi di identificazione personale Attività economiche, commerciali, finanziarie e assicurative
Unità di archiviazione della banca dati	
1 - Faldoni su scaffali (sede: Sede Principale azienda)	
<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati alla Sorveglianza</i>	<ul style="list-style-type: none"> ELVIO AROSIO

<i>degli archivi :</i>		
2 - Server (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	

Banca Dati : Corsi e formazione

Data anagrafici e di identificazione personale iscritti ai corsi, Registro presenze

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Istruzione e cultura
-------------------------------	--

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	

2 - Server (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	

Banca Dati : Curriculum

Mail, Lettere, Fax.

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Lavoro • Istruzione e cultura • Abitudini di vita o di consumo • Voti, giudizi ed altri dati di valutazione del rendimento scolastico
<i>Dati Sensibili trattati :</i>	<ul style="list-style-type: none"> • Origini razziali o etniche • Convinzioni religiose • Convinzioni filosofiche o di altro genere • Opinioni politiche • Adesione a partiti • Adesione a sindacati • Stato di salute • Vita sessuale

Unita' di archiviazione della banca dati		
1 - Faldoni su scaffali (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
2 - Server (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
Banca Dati : Gare e appalti		
Capitolati, bandi, offerte, documenti di partecipazione, visure camerali con diciture antimafia		
<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Attività economiche, commerciali, finanziarie e assicurative • Istruzione e cultura • Beni, proprietà, possessi 	
<i>Dati Giudiziari trattati :</i>	<ul style="list-style-type: none"> • Informazioni concernenti i provvedimenti giudiziari 	
Unita' di archiviazione della banca dati		
1 - Faldoni su scaffali (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
2 - Server (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	

Banca Dati : Gestione Personale

Dati anagrafici, Contratti, Corrispondenza, Fogli presenze, Libro matricole, Cud e documenti obbligatori per legge

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Lavoro • Istruzione e cultura • Voti, giudizi ed altri dati di valutazione del rendimento scolastico • Dati relativi al tipo di lavoro ed alla retribuzione
<i>Dati Sensibili trattati :</i>	<ul style="list-style-type: none"> • Origini razziali o etniche • Convinzioni religiose • Opinioni politiche • Adesione a partiti • Adesione a sindacati • Stato di salute • Log File di Navigazione Internet

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

2 - Server (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

Banca Dati : Marketing

Mail, Offerte, Fax, Rubriche

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative
-------------------------------	--

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

2 - Server (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)

	<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
	<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
	<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

Banca Dati : Posta elettronica

Mail, allegati, robriche

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Lavoro • Attività economiche, commerciali, finanziarie e assicurative • Istruzione e cultura • Beni, proprietà, possessi • Dati sul comportamento • Abitudini di vita o di consumo • Dati relativi allo svolgimento delle attività economiche dell'interessato. • Voti, giudizi ed altri dati di valutazione del rendimento scolastico • Dati relativi al tipo di lavoro ed alla retribuzione
<i>Dati Sensibili trattati :</i>	<ul style="list-style-type: none"> • Origini razziali o etniche • Convinzioni religiose • Convinzioni filosofiche o di altro genere • Opinioni politiche • Adesione a partiti • Adesione a sindacati • Stato di salute • Vita sessuale

Unita' di archiviazione della banca dati

1 - Server (sede: Sede Principale azienda)

	<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
	<i>Ufficio:</i>	Ufficio Direzionale
	<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
	<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
	<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
	<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

Banca Dati : Vendite

Dati anagrafici, Fatture, Ddt, Ordini, Preventivi, Documenti bancari, Rubriche, Corrispondenza, Rapporti di intervento (installazioni etc.)

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative
-------------------------------	--

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

	<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
	<i>Ufficio:</i>	Ufficio Direzionale
	<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
	<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

2 - Server (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

Banca Dati : Videosorveglianza

Filmati privi di audio.

<i>Dati Sensibili trattati :</i>	<ul style="list-style-type: none"> • RegISTRAZIONI di videosorveglianza
Unita' di archiviazione della banca dati	

1 - Pc Videosorveglianza (sede: Sale prove C/o Scuola Don Minzoni)

<i>Descrizione archivio:</i>	Prsonal Computer per Videosorveglianza
<i>Ufficio:</i>	Sala Attesa
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

Categorie di soggetti interessate al trattamento

Riportiamo ora in maggior dettaglio i trattamenti effettuati, distinguendo a quali soggetti interessati appartengono i dati oggetto di trattamento. Ulteriori informazioni a riguardo possono essere trovate, se previste, nelle relative informative.

Categoria di soggetti interessata : Candidati da considerare per l'instaurazione di un rapporto di lavoro

<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Curriculum • Posta elettronica
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Abitudini di vita o di consumo • Adesione a partiti • Adesione a sindacati • Codice fiscale ed altri numeri di identificazione personale • Convinzioni filosofiche o di altro genere • Convinzioni religiose • Dati relativi alla famiglia e a situazioni personali • Istruzione e cultura • Lavoro • Nominativo, indirizzo o altri elementi di identificazione personale • Opinioni politiche • Origini razziali o etniche • Stato di salute • Vita sessuale • Voti, giudizi ed altri dati di valutazione del rendimento scolastico
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Selezione del personale per l'instaurazione di un rapporto di lavoro
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei

Categoria di soggetti interessata : Clienti	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Vendite • Posta elettronica • Marketing
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Eventualmente per soddisfare indagini di mercato, statistiche e per attività promozionali inerenti anche alla spedizione di materiale pubblicitario e promozionale • Adempimenti obbligatori per legge in campo fiscale e contabile • Assistenza post-vendita • Gestione del contenzioso • Gestione della clientela • Gestione della Qualità • Programmazione delle attività • Rilevazione del grado di soddisfazione della clientela • Storico fatturazione clienti
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Affidamento a terzi di operazioni di elaborazione • Creazione di profili relativi a clienti, fornitori o consumatori • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Consulenti e liberi professionisti, anche in forma associata • Banche e istituti di credito • Spedizionieri, Trasportatori, Padroncini, Poste, Aziende per la Logistica
Categoria di soggetti interessata : Potenziali clienti	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Posta elettronica • Marketing
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Eventualmente per soddisfare indagini di mercato, statistiche e per attività promozionali inerenti anche alla spedizione di materiale pubblicitario e promozionale
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Elaborazione di dati raccolti da terzi • Raccolta di dati in luoghi pubblici o aperti al pubblico. • Raccolta di dati tramite schede, coupons e questionari. • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
Categoria di soggetti interessata : Fornitori	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Acquisti • Posta elettronica
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Adempimenti obbligatori per legge in campo fiscale e contabile • Gestione dei fornitori • Gestione del contenzioso • Gestione della Qualità • Di obblighi previsti dalle leggi vigenti • Programmazione delle attività • Storico ordini forniture
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Affidamento a terzi di operazioni di elaborazione • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Consulenti e liberi professionisti, anche in forma associata • Banche e istituti di credito • Nell'ambito di soggetti pubblici e/o privati per i quali la comunicazione dei dati è obbligatoria o necessaria in adempimento ad obblighi di legge o sia comunque

	<p>funzionale all'amministrazione del rapporto</p> <ul style="list-style-type: none"> • Spedizionieri, Trasportatori, Padroncini, Poste, Aziende per la Logistica
Categoria di soggetti interessata : Dipendenti e personale parasubordinato	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Gestione Personale
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Adesione a partiti • Adesione a sindacati • Codice fiscale ed altri numeri di identificazione personale • Convinzioni religiose • Dati relativi al tipo di lavoro ed alla retribuzione • Dati relativi alla famiglia e a situazioni personali • Istruzione e cultura • Lavoro • Log File di Navigazione Internet • Nominativo, indirizzo o altri elementi di identificazione personale • Opinioni politiche • Origini razziali o etniche • Stato di salute • Voti, giudizi ed altri dati di valutazione del rendimento scolastico
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali • Adempimenti obbligatori per legge in campo fiscale e contabile • Gestione del contenzioso • Gestione del personale in genere • Gestione della Qualità • Igiene e sicurezza del lavoro • Programmazione delle attività • Servizi di controllo interno • Trattamento giuridico ed economico del personale
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Affidamento a terzi di operazioni di elaborazione • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Organi costituzionali o di rilievo costituzionale • Enti previdenziali e assistenziali • Organizzazioni sindacali e patronati • Consulenti e liberi professionisti, anche in forma associata • Banche e istituti di credito • Imprese di assicurazione • Familiari dell'interessato
Categoria di soggetti interessata : Interessati Videosorveglianza	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Videosorveglianza
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • RegISTRAZIONI di videosorveglianza
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Servizio di controllo/sicurezza e Conservazione registrazioni per 24 ore
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Forze di polizia
Categoria di soggetti interessata : Corsisti	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Marketing • Corsi e formazione
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Istruzione e cultura • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Stesura relazione a committente

	<ul style="list-style-type: none"> • Compilazione attestati di frequenza • Gestione esercitazioni pratiche • Pianificazione attività dei corsi
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Committenti • Familiari dell'interessato • Subfornitori

Categoria di soggetti interessata : Socio e Società

<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Gare e appalti
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Beni, proprietà, possessi • Codice fiscale ed altri numeri di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Informazioni concernenti i provvedimenti giudiziari • Istruzione e cultura • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Presentazione di offerte per partecipazione a gare ed appalti
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Committenti

Categoria di soggetti interessata : Committenza

<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Gare e appalti
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Presentazione di offerte per partecipazione a gare ed appalti
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

Elenco dei soggetti autorizzati ad accedere agli archivi cartacei ad accesso controllato dopo l'orario di chiusura

Il punto 29 dell'allegato B prevede che i soggetti che accedono ad archivi cartacei contenenti dati sensibili o giudiziari dopo l'orario di chiusura siano preventivamente autorizzati, se non è possibile controllarne l'accesso con strumenti elettronici o con incaricati alla vigilanza.

Sono sotto riportati gli archivi per cui è previsto un accesso controllato dopo l'orario di chiusura e l'elenco dei soggetti autorizzati:

Faldoni su scaffali : Faldoni su scaffalatura a giorno in ferro e legno

Incaricati dopo l'orario di chiusura :

- ELVIO AROSIO



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

ANALISI DI RISCHIO E MISURE ADOTTATE

Scopo di questo documento di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali effettuato da GAIN STUDIOS DI AROSIO ELVIO S.A.S..

Rischi per ogni unità di archiviazione :

FALDONI SU SCAFFALI: Fattore di rischio = medio (6)

<i>Tipo di archivio</i>	Archivio cartaceo
<i>Tipi di dati contenuti</i>	dati sensibili, dati giudiziari, dati comuni
Rischi presenti	
<i>accesso non autorizzato ai dati cartacei</i>	Rischio Residuo = medio Livello di Copertura = molto basso
<i>Crollo Struttura</i>	Rischio Residuo = medio Livello di Copertura = nessuno
<i>Scrittura Dati errati</i>	Rischio Residuo = basso Livello di Copertura = basso
<i>Distruzione o Modifica volontaria dei Dati</i>	Rischio Residuo = basso Livello di Copertura = nessuno
<i>Incendio</i>	Rischio Residuo = basso Livello di Copertura = nessuno
<i>Divulgazione Intenzionale dei Dati</i>	Rischio Residuo = basso Livello di Copertura = nessuno
<i>Allagamento</i>	Rischio Residuo = basso Livello di Copertura = nessuno
<i>Distruzione o Modifica accidentale dei Dati</i>	Rischio Residuo = molto basso Livello di Copertura = alto
<i>Furti di Dati perpetrati da personale Interno</i>	Rischio Residuo = molto basso Livello di Copertura = medio
<i>Furti di Dati perpetrati dall'esterno</i>	Rischio Residuo = molto basso Livello di Copertura = alto
<i>Divulgazione accidentale dei Dati</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
Misure Adottate	
<i>Misure Fisiche</i>	<ul style="list-style-type: none"> • Installazione Allarme • Dotazione serrature ufficio. • Custodia in classificatori o armadi non accessibili. • Archivio ad accesso controllato. • Controllo dei documenti con dati sensibili o giudiziari da parte degli incaricati.
<i>Misure Organizzative</i>	<ul style="list-style-type: none"> • Redazione di un piano di formazione per gli incaricati. • Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione. • Consegna istruzioni dettagliate agli incaricati. <ul style="list-style-type: none"> • Istruzioni scritte finalizzate al controllo ed alla custodia dei documenti cartacei.

		<ul style="list-style-type: none"> E' stato redatto e viene annualmente aggiornato il documento Programmatico sulla sicurezza. Descrizione scritta degli interventi effettuati da terzi.
Nessuna misura prevista nel piano di miglioramento per questa unita' di archiviazione.		
PC VIDEOSORVEGLIANZA: Fattore di rischio = alto (12)		
<i>Tipo di archivio</i>	Archivio digitale su rete pubblica	
<i>Tipi di dati contenuti</i>	dati sensibili	
Rischi presenti		
	<i>Danno All'infrastruttura Hardware</i>	Rischio Residuo = molto alto Livello di Copertura = nessuno
	<i>Mancata erogazione elettrica</i>	Rischio Residuo = alto Livello di Copertura = nessuno
	<i>Divulgazione Intenzionale dei Dati</i>	Rischio Residuo = alto Livello di Copertura = nessuno
	<i>Guasto Hardware al supporto di Back-up</i>	Rischio Residuo = alto Livello di Copertura = nessuno
	<i>Guasto ai supporti di Back-up</i>	Rischio Residuo = alto Livello di Copertura = nessuno
	<i>Errore di salvataggio sui supporti di Back-up</i>	Rischio Residuo = alto Livello di Copertura = nessuno
	<i>Crollo Struttura</i>	Rischio Residuo = medio Livello di Copertura = nessuno
	<i>Corto Circuito elettrico</i>	Rischio Residuo = medio Livello di Copertura = nessuno
	<i>Caduta della Linea Trasmissione Dati</i>	Rischio Residuo = medio Livello di Copertura = nessuno
	<i>Accesso non autorizzato ai dati digitali</i>	Rischio Residuo = basso Livello di Copertura = basso
	<i>Intasamento Linea trasmissione dati</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Allagamento</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Incendio</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Caduta Rete Locale</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Furti di Dati perpetrati da personale Interno</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Furti di Dati perpetrati dall'esterno</i>	Rischio Residuo = basso Livello di Copertura = basso
	<i>Scrittura Dati errati</i>	Rischio Residuo = molto basso Livello di Copertura = alto
	<i>Interruzione temporanea all'uso dei dati</i>	Rischio Residuo = molto basso Livello di Copertura = alto
	<i>Distruzione o Modifica accidentale dei Dati</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Danni ai Programmi Software</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Presenza di Virus</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Divulgazione accidentale dei Dati</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Danno ai Dati</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Distruzione o Modifica</i>	Rischio Residuo = molto basso

	<i>volontaria dei Dati</i>	Livello di Copertura = molto alto
Misure Adottate		
	<i>Misure Fisiche</i>	<ul style="list-style-type: none"> • Installazione di un Firewall. <ul style="list-style-type: none"> • Firewall hardware. • Firewall software.
		<ul style="list-style-type: none"> • Copie di Back-up. <ul style="list-style-type: none"> • Back-Up su Disco Rigido. • Back-Up giornaliero. • Back-Up eseguito in Automatico. • Back-Up Completo. • Back-Up Sullo stesso supporto.
		<ul style="list-style-type: none"> • Antivirus. <ul style="list-style-type: none"> • Altri Antivirus. • Aggiornamento settimanale.
		<ul style="list-style-type: none"> • Credenziali di autenticazione, assegnate individualmente ad ogni incaricato. <ul style="list-style-type: none"> • Parola chiave di almeno 8 caratteri. • Disattivazione delle vecchie credenziali. • Disposizioni scritte per la disponibilità dei dati. • Autenticazione mediante user-id e password.
		<ul style="list-style-type: none"> • Sistema Operativo. <ul style="list-style-type: none"> • Windows XP Pro Edition.
		<ul style="list-style-type: none"> • Aggiornamento Software semestrale (annuale).
		<ul style="list-style-type: none"> • Profili di autorizzazione di ambito diverso per diversi incaricati. <ul style="list-style-type: none"> • E' utilizzato un sistema di autorizzazione. • I profili di autorizzazione vengono specificati prima di ogni trattamento. • Verifica periodica del profilo di autorizzazione.
	<i>Misure Organizzative</i>	<ul style="list-style-type: none"> • Redazione di un piano di formazione per gli incaricati.
		<ul style="list-style-type: none"> • Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione.
		<ul style="list-style-type: none"> • Consegna istruzioni dettagliate agli incaricati. <ul style="list-style-type: none"> • Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali. • Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento. • Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari.
		<ul style="list-style-type: none"> • Procedure per ripristino dei dati.
		<ul style="list-style-type: none"> • E' stato redatto e viene annualmente aggiornato il documento Programmatico sulla sicurezza.
		<ul style="list-style-type: none"> • Distruzione dei supporti removibili.
		<ul style="list-style-type: none"> • Descrizione scritta degli interventi effettuati da terzi.
Nessuna misura prevista nel piano di miglioramento per questa unita' di archiviazione.		

SERVER: Fattore di rischio = alto (12)

<i>Tipo di archivio</i>	Archivio digitale su rete pubblica
<i>Tipi di dati contenuti</i>	dati sensibili, dati giudiziari, dati comuni
Rischi presenti	
<i>Danno All'infrastruttura Hardware</i>	Rischio Residuo = molto alto Livello di Copertura = nessuno
<i>Mancata erogazione elettrica</i>	Rischio Residuo = alto Livello di Copertura = nessuno
<i>Divulgazione Intenzionale dei Dati</i>	Rischio Residuo = alto Livello di Copertura = nessuno
<i>Guasto Hardware al supporto di Back-up</i>	Rischio Residuo = alto Livello di Copertura = nessuno
<i>Guasto ai supporti di Back-up</i>	Rischio Residuo = alto Livello di Copertura = nessuno

	<i>Errore di salvataggio sui supporti di Back-up</i>	Rischio Residuo = alto Livello di Copertura = nessuno
	<i>Crollo Struttura</i>	Rischio Residuo = medio Livello di Copertura = nessuno
	<i>Corto Circuito elettrico</i>	Rischio Residuo = medio Livello di Copertura = nessuno
	<i>Caduta della Linea Trasmissione Dati</i>	Rischio Residuo = medio Livello di Copertura = nessuno
	<i>Accesso non autorizzato ai dati digitali</i>	Rischio Residuo = basso Livello di Copertura = basso
	<i>Intasamento Linea trasmissione dati</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Allagamento</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Incendio</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Caduta Rete Locale</i>	Rischio Residuo = basso Livello di Copertura = nessuno
	<i>Furti di Dati perpetrati da personale Interno</i>	Rischio Residuo = basso Livello di Copertura = basso
	<i>Scrittura Dati errati</i>	Rischio Residuo = molto basso Livello di Copertura = alto
	<i>Interruzione temporanea all'uso dei dati</i>	Rischio Residuo = molto basso Livello di Copertura = alto
	<i>Furti di Dati perpetrati dall'esterno</i>	Rischio Residuo = molto basso Livello di Copertura = medio
	<i>Presenza di Virus</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Danni ai Programmi Software</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Distruzione o Modifica accidentale dei Dati</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Divulgazione accidentale dei Dati</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Danno ai Dati</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
	<i>Distruzione o Modifica volontaria dei Dati</i>	Rischio Residuo = molto basso Livello di Copertura = molto alto
Misure Adottate		
	<i>Misure Fisiche</i>	<ul style="list-style-type: none"> • Installazione di un Firewall. <ul style="list-style-type: none"> • Firewall hardware. • Installazione Allarme • Dotazione serrature ufficio.
		<ul style="list-style-type: none"> • Copie di Back-up. <ul style="list-style-type: none"> • Back-Up su Nastro Magnetico. • Back-Up giornaliero. • Back-Up eseguito in Automatico. • Back-Up Completo. • Riutilizzo ciclico dei supporti ogni 7 volte.
		<ul style="list-style-type: none"> • Antivirus. <ul style="list-style-type: none"> • Altri Antivirus. • Aggiornamento settimanale.
		<ul style="list-style-type: none"> • Credenziali di autenticazione, assegnate individualmente ad ogni incaricato. <ul style="list-style-type: none"> • Parola chiave di almeno 8 caratteri. • Disattivazione delle vecchie credenziali. • Disposizioni scritte per la disponibilità dei dati.

		<ul style="list-style-type: none"> • Autenticazione mediante user-id e password.
		<ul style="list-style-type: none"> • Sistema Operativo. <ul style="list-style-type: none"> • Win2000 Server.
		<ul style="list-style-type: none"> • Aggiornamento Software semestrale (annuale).
		<ul style="list-style-type: none"> • Profili di autorizzazione di ambito diverso per diversi incaricati. <ul style="list-style-type: none"> • E' utilizzato un sistema di autorizzazione. • I profili di autorizzazione vengono specificati prima di ogni trattamento. • Verifica periodica del profilo di autorizzazione.
	<i>Misure Organizzative</i>	<ul style="list-style-type: none"> • Redazione di un piano di formazione per gli incaricati.
		<ul style="list-style-type: none"> • Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione.
		<ul style="list-style-type: none"> • Consegna istruzioni dettagliate agli incaricati. <ul style="list-style-type: none"> • Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali. • Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento. • Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari.
		<ul style="list-style-type: none"> • Procedure per ripristino dei dati.
		<ul style="list-style-type: none"> • E' stato redatto e viene annualmente aggiornato il documento Programmatico sulla sicurezza.
		<ul style="list-style-type: none"> • Distruzione dei supporti removibili.
		<ul style="list-style-type: none"> • Descrizione scritta degli interventi effettuati da terzi.
Misure Previste per il Piano di Miglioramento		
	<i>Misure Fisiche</i>	<ul style="list-style-type: none"> • Gruppo di continuità



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

RIPRISTINO DEI DATI

Descrizione dei criteri attuati per garantire il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento.

Sistemi di elaborazione

Pc Videosorveglianza

<i>Tipi di dato presenti</i>	dati sensibili
Criticita' dei dati	media
<i>Responsabili della strumentazione elettronica</i>	ELVIO AROSIO
<i>Incaricati alla gestione del sistema di elaborazione</i>	ELVIO AROSIO
<i>Incaricati ai back-up</i>	ELVIO AROSIO
<i>Responsabili o consulenti esterni da contattare in caso di emergenza</i>	Studio di Informatica Maraschi
<i>Fornitori che possono fornire apparecchiature sostitutive in caso di guasto</i>	Studio di Informatica Maraschi
<i>Frequenza di back-up</i>	Back-Up giornaliero.
<i>Tipo di supporto per il back-up</i>	Back-Up su Disco Rigido.
<i>Tipo di back-up</i>	Back-Up Completo.
<i>Modalita' di back-up</i>	Back-Up eseguito in Automatico.
<i>Riutilizzo dei supporti</i>	Back-Up Sullo stesso supporto.
<i>Eventuale software utilizzato</i>	Backup di Microsoft
<i>Tempo di Ripristino</i>	minore di 7 giorni
<i>Procedura per il ripristino</i>	Per il ripristino vengono eseguite le procedure indicate dalla manualistica del produttore del software

Server

<i>Tipi di dato presenti</i>	dati sensibili, dati giudiziari, dati comuni
Criticita' dei dati	alta
<i>Responsabili della strumentazione elettronica</i>	ELVIO AROSIO
<i>Incaricati alla gestione del sistema di elaborazione</i>	ELVIO AROSIO
<i>Incaricati ai back-up</i>	ELVIO AROSIO
<i>Responsabili o consulenti esterni da contattare in caso di emergenza</i>	Studio di Informatica Maraschi

<i>Fornitori che possono fornire apparecchiature sostitutive in caso di guasto</i>	Studio di Informatica Maraschi
<i>Frequenza di back-up</i>	Back-Up giornaliero.
<i>Tipo di supporto per il back-up</i>	Back-Up su Nastro Magnetico.
<i>Tipo di back-up</i>	Back-Up Completo.
<i>Modalita' di back-up</i>	Back-Up eseguito in Automatico.
<i>Riutilizzo dei supporti</i>	Riutilizzo ciclico dei supporti ogni 7 volte.
<i>Eventuale software utilizzato</i>	Backup di Microsoft
<i>Tempo di Ripristino</i>	minore di 7 giorni
<i>Procedura per il ripristino</i>	Per il ripristino vengono eseguite le procedure indicate dalla manualistica del produttore del software



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

PIANO DI FORMAZIONE

Elenco degli interventi formativi effettuati o progettati per gli incaricati e per i responsabili della Privacy.

Interventi formativi

ELVIO AROSIO

29/12/2008 : Aggiornamento della Nomina e consegna delle istruzioni e dei compiti, dettagliati e personalizzati, per la corretta gestione della Privacy.

Formazione per i nuovi incaricati

Nel caso di un nuovo incaricato, è prevista la seguente formazione prima dell'inizio del trattamento: Assegnazione di dettagliate istruzioni scritte e personalizzate, complete dell'ambito di trattamento del nuovo incaricato, e formazione orale sugli obblighi di legge e sulle norme di condotta da parte del titolare o del responsabile al trattamento.

Formazione prevista nel caso di cambiamenti di mansioni

Nel caso in cui siano affidate mansioni differenti ad un incaricato, è prevista la seguente formazione: Assegnazione di istruzioni scritte aggiornate e complete relative al nuovo trattamento.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

ELENCO DEI TRATTAMENTI ESTERNI

Elenco dei trattamenti esterni dei dati e dei criteri adottati per garantire il rispetto delle misure minime di sicurezza da parte dei titolari esterni.

Affidatario del Trattamento : Studio Associato Pomati Schiavi Manera - P.zza Botta 1, 27100 Pavia

Finalità del Trattamento : adempimenti ad obblighi di legge in materia fiscale e contabile

I dati affidati all'esterno fanno riferimento alle seguenti banche dati : Acquisti, Vendite, Gare e appalti

Criterio adottato per garantire il rispetto delle misure di sicurezza : La dichiarazione scritta, da parte dell'affidatario, su carta intestata, di avere adottato le misure minime previste dalla legge.

Affidatario del Trattamento : Studio CDL Associati - via Torchietto 4, 27100 Pavia

Finalità del Trattamento : consulenza in materia di lavoro e gestione paghe e contributi

I dati affidati all'esterno fanno riferimento alle seguenti banche dati : Gestione Personale, Curriculum

Criterio adottato per garantire il rispetto delle misure di sicurezza : La dichiarazione scritta, da parte dell'affidatario, su carta intestata, di avere adottato le misure minime previste dalla legge.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

Elenco delle Misure Minime

Sono sotto riportate le misure minime che devono essere implementate, così come specificato negli artt. da 33 a 36 del codice e dall'Allegato B. La mancata implementazione delle misure minime può comportare sanzioni penali fino ai due anni di arresto oppure sanzioni amministrative fino a 50.000 euro. Il presente documento si basa sui tipi di dati e sulle unità di archiviazione riportati nell'organigramma, ed è da considerare corretto se tali dati sono stati inseriti in modo completo. Il presente documento è esclusivamente ad uso interno dell'azienda, nel senso che il codice della privacy non richiede che sia stampato o conservato in azienda, ma può essere utile per avere un riferimento chiaro su quali siano le misure minime da adottare.

Misure Minime da adottare a livello organizzativo

Misure Minime	
<i>Implementata</i>	<ul style="list-style-type: none"> Descrizione scritta degli interventi effettuati da terzi. Quando ci si avvale di soggetti esterni per l'adozione pratica delle misure di sicurezza minima, si richiede la descrizione scritta dell'intervento effettuato che ne attesta la conformità a norma di legge.
<i>Implementata</i>	<ul style="list-style-type: none"> Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione. Periodicamente, con cadenza almeno annuale, sono aggiornati gli ambiti del trattamento consentito agli incaricati ed agli addetti alla gestione o manutenzione dei sistemi elettronici.
<i>Implementata</i>	<ul style="list-style-type: none"> Consegna istruzioni dettagliate agli incaricati. Ad ogni incaricato sono state consegnate istruzioni dettagliate e complete riguardanti il trattamento dei dati personali, a seconda dei suoi compiti e dei dati trattati. <ul style="list-style-type: none"> Implementata: Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali. Implementata: Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento. Implementata: Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari. Implementata: Istruzioni scritte finalizzate al controllo ed alla custodia dei documenti cartacei.
DA IMPLEMENTARE	<ul style="list-style-type: none"> Inserimento nella relazione accompagnatoria del bilancio d'esercizio della redazione o aggiornamento del DPSS. Le Aziende, gli Enti, le Associazioni che hanno l'obbligo di redigere la relazione accompagnatoria al bilancio devono inserire nella stessa se e quando è stato redatto il Documento Programmatico sulla Sicurezza. Chi non deve redigere la relazione accompagnatoria al bilancio è esentato rispetto a questa misura minima.
<i>Implementata</i>	<ul style="list-style-type: none"> E' stato redatto e viene annualmente aggiornato il documento Programmatico sulla sicurezza. Il DPSS è obbligatorio solo se si trattano dati sensibili o giudiziari su elaboratori elettronici.
<i>Implementata</i>	<ul style="list-style-type: none"> Distruzione dei supporti removibili. Nel caso di dati sensibili o giudiziari, i supporti rimuovibili che contengono tali dati se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere usati da personale non autorizzato solo dopo che i dati in essi contenuti sono resi non intelleggibili e tecnicamente in alcun modo recuperabili.
<i>Implementata</i>	<ul style="list-style-type: none"> Redazione di un piano di formazione per gli incaricati. E' previsto un piano di formazione degli incaricati, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevedere eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti,

		rilevanti rispetto al trattamento dei dati personali.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Procedure per ripristino dei dati. Sono state adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori ai 7 giorni.
Misure Minime da adottare per ogni unità di archiviazione		
FALDONI SU SCAFFALI		
<i>Tipo di archivio</i>	Archivio cartaceo	
<i>Tipi di dati contenuti</i>	dati sensibili, dati giudiziari, dati comuni	
Misure Minime		
	<i>DA IMPLEMENTARE</i>	<ul style="list-style-type: none"> • Dotazione di serrature per l'archivio o per l'ufficio. Se sono presenti dati sensibili o giudiziari ed archivi cartacei, è necessaria una chiusura a chiave o dell'ufficio o dell'archivio.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Archivio ad accesso controllato. L'accesso all'archivio è controllato dagli incaricati al trattamento o dalla sorveglianza. Dopo l'orario di chiusura possono accedere all'archivio solo le persone preventivamente autorizzate od identificate e registrate.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Controllo dei documenti con dati sensibili o giudiziari da parte degli incaricati. Quando i documenti contenenti dati sensibili o giudiziari sono affidati agli incaricati del trattamento, i medesimi atti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Custodia in classificatori o armadi non accessibili. I dati cartacei sono archiviati in modo da permettere l'accesso esclusivamente agli incaricati al trattamento degli stessi e di non essere accessibili a persone non autorizzate.
PC VIDEOSORVEGLIANZA		
<i>Tipo di archivio</i>	Archivio digitale su rete pubblica	
<i>Tipi di dati contenuti</i>	dati sensibili	
Misure Minime		
	<i>Implementata</i>	<ul style="list-style-type: none"> • Sistema Operativo. Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli incaricati al trattamento dei dati. Specificare il sistema operativo installato sul sistema. <ul style="list-style-type: none"> • Implementata: Windows XP Pro Edition.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Copie di Back-up. Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. <ul style="list-style-type: none"> • Implementata: Back-Up giornaliero.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Antivirus. Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente (od annualmente nel caso in cui contengano solo dati comuni). <ul style="list-style-type: none"> • Implementata: Aggiornamento settimanale.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Credenziali di autenticazione, assegnate individualmente ad ogni incaricato. Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione univocamente associata all'incaricato e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri incaricati, nemmeno in tempi diversi. <ul style="list-style-type: none"> • Implementata: Parola chiave di almeno 8 caratteri. • Implementata: Disattivazione delle vecchie credenziali. • Implementata: Disposizioni scritte per la disponibilità dei dati. • Implementata: Autenticazione mediante user-id e password.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Profili di autorizzazione di ambito diverso per diversi incaricati. Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato.

		<ul style="list-style-type: none"> • Implementata: E' utilizzato un sistema di autorizzazione. • Implementata: I profili di autorizzazione vengono specificati prima di ogni trattamento. • Implementata: Verifica periodica del profilo di autorizzazione.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Aggiornamento Software semestrale (annuale). Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati semestralmente (od annualmente se sono presenti solo dati comuni).
	<i>Implementata</i>	<ul style="list-style-type: none"> • Installazione di un Firewall. Nel caso di trattamento di dati sensibili o giudiziari con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. <ul style="list-style-type: none"> • Implementata: Firewall hardware. • Implementata: Firewall software.

SERVER

<i>Tipo di archivio</i>	Archivio digitale su rete pubblica	
<i>Tipi di dati contenuti</i>	dati sensibili, dati giudiziari, dati comuni	
Misure Minime		
	<i>Implementata</i>	<ul style="list-style-type: none"> • Sistema Operativo. Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli incaricati al trattamento dei dati. Specificare il sistema operativo installato sul sistema. <ul style="list-style-type: none"> • Implementata: Win2000 Server.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Copie di Back-up. Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. <ul style="list-style-type: none"> • Implementata: Back-Up giornaliero.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Antivirus. Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente (od annualmente nel caso in cui contengano solo dati comuni). <ul style="list-style-type: none"> • Implementata: Aggiornamento settimanale.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Credenziali di autenticazione, assegnate individualmente ad ogni incaricato. Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione univocamente associata all'incaricato e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri incaricati, nemmeno in tempi diversi. <ul style="list-style-type: none"> • Implementata: Parola chiave di almeno 8 caratteri. • Implementata: Disattivazione delle vecchie credenziali. • Implementata: Disposizioni scritte per la disponibilità dei dati. • Implementata: Autenticazione mediante user-id e password.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Profili di autorizzazione di ambito diverso per diversi incaricati. Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. <ul style="list-style-type: none"> • Implementata: E' utilizzato un sistema di autorizzazione. • Implementata: I profili di autorizzazione vengono specificati prima di ogni trattamento. • Implementata: Verifica periodica del profilo di autorizzazione.
	<i>Implementata</i>	<ul style="list-style-type: none"> • Aggiornamento Software semestrale (annuale). Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati semestralmente (od annualmente se sono presenti solo dati comuni).
	<i>Implementata</i>	<ul style="list-style-type: none"> • Installazione di un Firewall. Nel caso di trattamento di dati sensibili o giudiziari con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. <ul style="list-style-type: none"> • Implementata: Firewall hardware.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

Compiti del responsabile

La Legge definisce come responsabile "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali".

I confini generali di tale ruolo vengono delineati dal combinato disposto degli articoli 4 e 29 del codice, ai sensi dei quali si definisce responsabile il soggetto preposto dal titolare al trattamento dei dati personali, che deve essere individuato tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Tale soggetto deve quindi possedere una competenza insieme tecnica, legale in materia di privacy ed organizzativa.

Trattamento dei dati

L'area 'trattamento dati' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni inerenti alla gestione dei rapporti tra il Titolare e il Garante, tra il Titolare e gli interessati, e alla gestione operativa dei trattamenti dei dati personali:

- gestione notifica
- gestione rapporti con il Garante
- verifica corrispondenza con Autorizzazioni Annuali
- gestione comunicazione e diffusione dei dati secondo legge
- gestione informativa e consenso verso interessati
- gestione diritti di accesso degli interessati
- gestione delle modalità dei trattamenti interni
- nomina degli incaricati del trattamento
- creazione e gestione dei profili di autorizzazione
- gestione dei trattamenti affidati a terzi
- gestione della formazione da impartire agli incaricati

È compito del Responsabile ai Trattamenti:

- Raggiungere un sufficiente grado di apprendimento in materia di Privacy in modo da poter trattare i dati secondo la Legge e realmente vigilare sulla liceità e sulla correttezza dei trattamenti.
- Predisporre la notificazione iniziale al Garante nel caso in cui il trattamento rientri nei casi contemplati dall'art.37 del Codice, attraverso il programma Web disponibile sul sito del Garante (www.garanteprivacy.it), verificando l'esattezza e la completezza dei dati contenuti.
- Interagire con il Garante, in caso di richieste di informazioni o effettuazione di controlli ed accessi da parte dell'autorità;
- Collaborare con eventuali altri Responsabili e con l'eventuale Amministratore di Sistema.
- Censire analiticamente le banche dati con tutti gli elementi necessari per la determinazione dei trattamenti e delle tipologie di dati da inserire nel DPSS (dati trattati, tipi di trattamento, categorie di interessati, sedi e uffici del trattamento e in collaborazione con il Responsabile della Sicurezza, l'elenco dei sistemi di elaborazione nei quali avvengono i trattamenti), anche ai fini della eventuale notifica al Garante;
- Verificare che i trattamenti dei dati sensibili rientrino nelle Autorizzazioni del Garante in corso di validità ed, eventualmente, predisporre la richiesta di autorizzazione preventiva al trattamento di dati sensibili nel caso in cui il trattamento non rientri in tali Autorizzazioni.
- Procedere alla gestione delle informative e delle richieste di consenso nei casi e nelle modalità previste dalla legge
- Aggiornare l'elenco dei trattamenti in relazione ad eventuali nuovi trattamenti di dati personali;
- Individuare e nominare gli incaricati del trattamento impartendo loro, per iscritto, la nomina, le istruzioni e le autorizzazioni necessarie ad un corretto, lecito e sicuro trattamento, verificandone la puntuale applicazione;
- Produrre le nomine, le istruzioni e la distribuzione dei compiti (mansionario privacy) da consegnare ai medesimi per la firma e l'archiviazione.
- Definire i profili di autorizzazione (ambiti di competenza e operazioni consentite) degli incaricati
- Autorizzare i singoli incaricati al trattamento specifico di dati sensibili e giudiziari ponendo bene in evidenza tale fatto nella definizione del profilo di autorizzazione;
- Tenere aggiornato l'elenco dei trattamenti (censimento delle banche dati, tipologie di dati trattati, sedi in cui vengono

- trattati) e la distribuzione dei compiti (mansionario della privacy), con cadenza almeno annuale.
- Periodicamente con cadenza almeno annuale verificare la correttezza dei profili di autorizzazione revisionando gli ambiti di competenza ed eventualmente adattandoli a nuove esigenze.
 - Provvedere a eliminare le autorizzazioni che rimangono inutilizzate oltre i sei mesi, sempre che il profilo particolare non determini per propria definizione un trattamento sporadico.
 - Attuare gli obblighi di informazione ad acquisizione del consenso, quando richiesto, nei confronti degli interessati; delegare eventualmente questa incombenza ai singoli incaricati. A tal fine è possibile utilizzare i moduli e le procedure predisposte attraverso il Portale della Privacy.
 - Individuare i trattamenti che vengono ceduti a Terzi (ad es. la gestione delle paghe) e attuare i necessari provvedimenti affinché tali trattamenti avvengano secondo liceità e correttezza garantendo lo standard di sicurezza previsto dalla legge. Il Responsabile deve decidere se nominare Responsabile la società terza in oggetto, se nominare Incaricati i soggetti individuali terzi che materialmente effettueranno i trattamenti o se introdurre restrittive clausole di garanzia nel contratto di fornitura del servizio. In queste operazioni può collaborare con l'eventuale Responsabile dell'area sicurezza.
 - Verificare che tutti i trattamenti avvengano nel rispetto delle disposizioni di legge.
 - Distruggere i dati personali che non sono più oggetto di trattamento alcuno.
 - Informare prontamente il Titolare ed il personale interno addetto alla privacy di ogni questione rilevante ai fini di legge;
 - Comunicare al Titolare qualsiasi elemento oggettivo o soggettivo che possa compromettere il corretto trattamento dei dati personali.
 - Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del Titolare; nel caso venga delegato il trattamento all'esterno gestire il trattamento tramite terzi attuando le misure necessarie affinché sia garantita la sicurezza dei dati esportati, questo anche in collaborazione con l'eventuale Responsabile dell'area sicurezza.
 - Collaborare con l'eventuale Responsabile dell'area sicurezza e con l'eventuale Amministratore di Sistema nella definizione delle credenziali di autenticazione e dei profili di autorizzazione.
 - Elaborare un piano di formazione per rendere edotti gli incaricati del trattamento delle disposizioni di legge sulle modalità e i criteri del trattamento, nonché dei rischi individuati e dei modi per prevenire danni, anche in collaborazione con gli altri Responsabili.
 - Collaborare con tutti i responsabili per l'attuazione delle prescrizioni impartite dal Garante attraverso nuove circolari, autorizzazioni e aggiornamenti di Legge;
 - Gestire la cifratura e la separazione nei casi in cui vi sia la coesistenza di dati identificativi dell'interessato e dati sensibili, con particolare riferimento a quelli sanitari, che consentano una immediata associazione tra di essi. E' possibile fare riferimento alle soluzioni proposte dal Portale della Privacy.

Sicurezza

L'area 'sicurezza' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni inerenti alla implementazione delle misure di sicurezza atte a proteggere in modo preventivo e idoneo (art. 31 del Codice) i dati personali oggetto di trattamento e, in particolare, delle Misure Minime di Sicurezza trattate dagli artt. 33, 34, 35, 36 e dall'Allegato Disciplinare Tecnico B, ponendo estrema attenzione ai trattamenti di dati sensibili e giudiziari:

E' compito del Responsabile individuare e nominare, se lo ritiene opportuno, un Amministratore di Sistema ed eventualmente un incaricato alla custodia delle copie credenziali. E' altresì suo compito nominare eventualmente un incaricato al controllo degli accessi ai locali e obbligatoriamente un incaricato alla sorveglianza dell'archivio ad accesso autorizzato se dovessero esistere all'interno della struttura del Titolare archivi cartacei o contenitori di supporti informatici rimuovibili, contenenti dati sensibili o giudiziari.

Se il Responsabile della sicurezza decidesse di non nominare nessun amministratore di sistema od incaricato, se ne assumerà interamente le funzioni, i compiti e le responsabilità in relazione alla sicurezza dei dati personali.

È compito del Responsabile della Sicurezza:

- Se il trattamento dei dati personali è effettuato con l'ausilio di strumenti informatici, censire tutti i sistemi di elaborazione elettronica indicandone le caratteristiche principali (sistemi operativi, gestione multiprofilo, programmi di protezione, sistemi di antintrusione, programmi di elaborazione dei dati) e aggiornare, con cadenza annuale, l'elenco di tali sistemi.
- Individuare la dislocazione fisica dei trattamenti e in particolare:
 - le aree e i locali nei quali si trovano gli elaboratori o i sistemi di accesso remoto alle banche dati elettroniche e in particolare i sistemi che consentono l'accesso a dati sensibili o giudiziari; per tali aree e locali è bene nominare un incaricato al controllo accessi.
 - gli uffici e gli archivi nei quali vengono trattati e riposti dati sensibili o giudiziari; per tali archivi è necessario nominare un incaricato alla sorveglianza.
- Definire e verificare le modalità di accesso a tali locali e le misure da adottare per la protezione dei medesimi:
 - predisponendo i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati nonché le procedure per controllare l'accesso delle persone autorizzate;
 - impartendo specifiche istruzioni agli incaricati al controllo e alla sorveglianza delle aree e dei locali nonché degli archivi contenenti dati sensibili o giudiziari.
- Rendere esecutive tutte le misure di sicurezza adottate per la protezione dei dati personali e verificare la loro corretta implementazione con cadenza, almeno, semestrale.
- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate anche all'esterno nel caso venga affidato a terzi il trattamento dei propri dati personali; collaborare in tal senso con il Responsabile all'area 'trattamento

dati' che ha compiti specifici.

- Predisporre ed aggiornare, entro il 31 Marzo di ogni anno, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi e produrre un piano di miglioramento incrementale di sicurezza (risk management) anche in base alle innovazioni tecnologiche in materia di protezione dei sistemi di elaborazione automatica e delle reti informatiche;
- Definire i criteri e le procedure per la sicurezza delle trasmissioni dei dati siano esse fatte attraverso fax o posta elettronica, ivi compresi quelli per le restrizioni di accesso per via telematica;
- Definire la politica di accesso alla rete da parte dei dipendenti, le loro responsabilità e le restrizioni in ordine alla sicurezza. Raccogliere, eventualmente, presso i dipendenti una assunzione di responsabilità per i siti visitati, nel caso venga loro concesso di navigare per proprio ed esclusivo interesse durante l'orario di lavoro.
- Relativamente alle disposizioni del punto precedente, è opportuno definire le modalità di gestione dei files di LOG da parte della direzione, fornendo a tal proposito espressa informativa e richiesta di consenso al trattamento dei medesimi: è da considerare il fatto che nei file di log siano contenuti dati personali anche sensibili. La direzione deve tenere in considerazione che il controllo dei log files rientra nelle disposizioni contenute nello Statuto dei Lavoratori art. 4 (Sorveglianza sul posto di lavoro).
- Custodire i supporti informatici adibiti alle copie di sicurezza dei dati impartendo istruzioni all'Amministratore di Sistema o all'incaricato della gestione e della manutenzione del sistema.
- Pianificare ed eseguire di test del sistema di sicurezza, attraverso adeguate prove di penetrazione
- Definire ed attuare di piani e strumenti di monitoraggio continuo della sicurezza
- Aggiornare periodicamente il sistema di sicurezza, per renderlo sempre adeguato alle nuove minacce
- Mantenere il sistema di sicurezza, per assicurarne costante efficienza e disponibilità
- Fornire supporto alla formazione del personale dell'organizzazione, in tema di sicurezza
- Emanare procedure interne inerenti la sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, ecc).
- Distruggere in modo definitivo i supporti rimovibili informatici destinati ad essere cestinati con particolare attenzione a quelli che contenevano dati personali sensibili;
- Distruggere le memorie fisse (Hard Disk) dei PC che eventualmente vanno in rottamazione.

Gestione dei sistemi di elaborazione elettronica.

L'area 'sistemi di elaborazione elettronica' comprende l'espletamento di tutte le operazioni inerenti alla gestione e alla manutenzione del sistema informatico non solo in rapporto alle soluzioni tecnologiche ma anche in ordine alle disposizioni di Legge in materia di sicurezza dei dati.

È compito del Responsabile individuare e nominare, se lo ritiene opportuno, uno o più incaricati alla manutenzione del sistema. Deve collaborare con gli altri responsabili nell'individuare e nominare gli incaricati al Back-up dei dati personali.

Se il Responsabile decidesse di non nominare nessun incaricato se ne assumerà le funzioni, i compiti e le responsabilità interamente.

È compito del Responsabile:

- Se il trattamento avviene con l'ausilio di mezzi informatici, deve redigere e aggiornare l'elenco dei sistemi hardware e software interessati al trattamento dei dati personali
- Attivare e gestire le credenziali di autenticazione degli incaricati ai trattamenti collaborando col Responsabile all'area 'trattamento dati' e col Responsabile alla sicurezza.
- Istruire gli incaricati dei trattamenti sull'uso delle parole chiave e sulle modalità per la modifica in autonomia, facendo riferimento al punto 3 delle istruzioni per l'incaricato dei trattamenti.
- Revocare e disattivare le credenziali di autenticazione agli incaricati che per qualunque motivo perdano la loro qualifica di incaricato
- Collaborare con il responsabile del trattamento nella definizione dei profili di autorizzazione definendo i trattamenti consentiti.
- Definire le politiche di protezione dei sistemi verso l'attacco di programmi (Virus) per tutte le basi dati elettroniche;
- Installare su tutte le postazioni client, sui server, sui PC e dove necessario (limitatamente all'ambito di competenza a lei assegnato) gli antivirus e aggiornarli con cadenza almeno semestrale! Si consiglia una frequenza del tutto più restrittiva.
- Effettuare tutti gli aggiornamenti patch dei sistemi operativi e dei programmi utilizzati per il trattamento dati, con cadenza annuale che diviene semestrale in caso di trattamenti di dati sensibili o giudiziari.
- Definire le politiche di protezione passiva della rete (firewall e sua configurazione) per la difesa del sistema dall'attacco di hackers.
- Verificare l'efficacia delle politiche di sicurezza almeno con cadenza semestrale.
- Collaborare con gli altri responsabili mantenendoli informati della gestione e di eventuali anomalie di sistema che potrebbero compromettere la sicurezza.
- Istruire gli incaricati dei back-up riguardo alle procedure da adottare per le operazioni di salvataggio delle copie di sicurezza dei dati personali, redigendo apposito documento di istruzioni. Risolvere gli eventuali problemi tecnici nella realizzazione dei back-up rilevati dai rispettivi incaricati.
- Sottoscrivere il documento con le istruzioni per il back up, conservarlo in luogo sicuro e trasmetterlo in copia agli incaricati del trattamento dei dati interessati alle copie di salvataggio, nonché all'incaricato dei back up di quella base dati.

Per ogni base dati deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up e le modalità di custodia.

- Istruire l'incaricato alla manutenzione del sistema affinché le operazioni di riparazione e ripristino avvengano nel rispetto delle disposizioni di legge: in particolare dovrà attivare le necessarie azioni previste in caso gli elaboratori vengano spediti verso altra struttura per essere sottoposti alle necessarie riparazioni (vedi Trattamento terzi, clausole contrattuali) anche in collaborazione con il Responsabile dei trattamenti.

Rapporto con gli Interessati

L'area 'rapporto con gli interessati' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni volte a soddisfare i diritti sanciti dall'art.7 del Codice della privacy.

È compito del Responsabile:

- Conoscere i modi e i tempi entro i quali venire incontro alle richieste dell'interessato (artt.7, 8, 146).
- Prendere in carico tempestivamente e non oltre le 24 ore successive al loro ricevimento, i reclami degli interessati e le eventuali istanze del garante.
- Effettuare la ricerca dei dati richiesti, producendone una copia rispondente ai criteri di intelleggibilità e chiarezza stabiliti dalla legge.
- Informare il titolare nel caso in cui dovessero intervenire delle difficoltà nella raccolta dei dati tali da compromettere in parte o del tutto la buona riuscita dell'operazione.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

Atto di Nomina dell'incaricato

Ai sensi e per gli effetti del D.Lgs. 30 Giugno 2003 n. 196

GAIN STUDIOS DI AROSIO ELVIO S.A.S. nella persona di ELVIO AROSIO in qualità di 'Titolare del Trattamento' dei dati personali, ai sensi e per gli effetti del art. 30 del D.Lgs. 30 Giugno 2003 n. 196 con il presente atto NOMINA :

Il Sig./Sig.ra ELVIO AROSIO

INCARICATO del trattamento dei dati personali.

Tale nomina è in relazione alle operazioni di elaborazione di dati personali ai quali i soggetti incaricati hanno accesso nell'espletamento della funzione che è loro propria. In particolare non è consentito l'accesso a dati la cui conoscenza non è necessaria all'adempimento dei compiti affidati agli incaricati. In ottemperanza al Codice della Privacy, che regola il trattamento dei dati personali, laddove costituisce trattamento "qualunque operazione o complesso di operazioni, effettuati 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 di dati".

L'ambito di applicazione della presente nomina fa riferimento ai tipi di dati ed alle mansioni sotto elencate:

Incaricato al trattamento dei dati personali.

Acquisti

Tipi di Dati : Dati Comuni

- Attività economiche, commerciali, finanziarie e assicurative
- Codice fiscale ed altri numeri di identificazione personale
- Nominativo, indirizzo o altri elementi di identificazione personale

Corsi e formazione

Tipi di Dati : Dati Comuni

- Codice fiscale ed altri numeri di identificazione personale
- Istruzione e cultura
- Nominativo, indirizzo o altri elementi di identificazione personale

Curriculum

Tipi di Dati : Dati Comuni

- Abitudini di vita o di consumo
- Codice fiscale ed altri numeri di identificazione personale
- Dati relativi alla famiglia e a situazioni personali
- Istruzione e cultura
- Lavoro
- Nominativo, indirizzo o altri elementi di identificazione personale
- Voti, giudizi ed altri dati di valutazione del rendimento scolastico

Tipi di Dati : Dati Sensibili

- Adesione a partiti
- Adesione a sindacati
- Convinzioni filosofiche o di altro genere
- Convinzioni religiose
- Opinioni politiche
- Origini razziali o etniche
- Stato di salute
- Vita sessuale

Gare e appalti

Tipi di Dati : Dati Comuni

- Attività economiche, commerciali, finanziarie e assicurative
- Beni, proprietà, possessi
- Codice fiscale ed altri numeri di identificazione personale
- Dati relativi alla famiglia e a situazioni personali
- Istruzione e cultura

		<ul style="list-style-type: none"> • Nominativo, indirizzo o altri elementi di identificazione personale
	<i>Tipi di Dati : Dati Giudiziari</i>	<ul style="list-style-type: none"> • Informazioni concernenti i provvedimenti giudiziari
Gestione Personale		
	<i>Tipi di Dati : Dati Comuni</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Dati relativi al tipo di lavoro ed alla retribuzione • Dati relativi alla famiglia e a situazioni personali • Istruzione e cultura • Lavoro • Nominativo, indirizzo o altri elementi di identificazione personale • Voti, giudizi ed altri dati di valutazione del rendimento scolastico
	<i>Tipi di Dati : Dati Sensibili</i>	<ul style="list-style-type: none"> • Adesione a partiti • Adesione a sindacati • Convinzioni religiose • Log File di Navigazione Internet • Opinioni politiche • Origini razziali o etniche • Stato di salute
Marketing		
	<i>Tipi di Dati : Dati Comuni</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
Posta elettronica		
	<i>Tipi di Dati : Dati Comuni</i>	<ul style="list-style-type: none"> • Abitudini di vita o di consumo • Attività economiche, commerciali, finanziarie e assicurative • Beni, proprietà, possessi • Codice fiscale ed altri numeri di identificazione personale • Dati relativi al tipo di lavoro ed alla retribuzione • Dati relativi alla famiglia e a situazioni personali • Dati relativi allo svolgimento delle attività economiche dell'interessato. • Dati sul comportamento • Istruzione e cultura • Lavoro • Nominativo, indirizzo o altri elementi di identificazione personale • Voti, giudizi ed altri dati di valutazione del rendimento scolastico
	<i>Tipi di Dati : Dati Sensibili</i>	<ul style="list-style-type: none"> • Adesione a partiti • Adesione a sindacati • Convinzioni filosofiche o di altro genere • Convinzioni religiose • Opinioni politiche • Origini razziali o etniche • Stato di salute • Vita sessuale
Vendite		
	<i>Tipi di Dati : Dati Comuni</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
Videosorveglianza		
	<i>Tipi di Dati : Dati Sensibili</i>	<ul style="list-style-type: none"> • Registrazioni di videosorveglianza
Incaricato al 'back-up' dei dati personali.		
<i>E' incaricato al back-up per le seguenti unità di elaborazione:</i>		<ul style="list-style-type: none"> • Pc Videosorveglianza • Server
Amministratore di sistema.		
<i>E' incaricato dell'amministrazione del</i>		<ul style="list-style-type: none"> • Pc Videosorveglianza • Server

<i>sistema per le seguenti unità di elaborazione:</i>	
Custode delle copie credenziali.	
<i>E' incaricato alla custodia delle copie credenziali per le seguenti unità di elaborazione:</i>	<ul style="list-style-type: none"> • Pc Videosorveglianza • Server
Sorveglianza degli archivi ad accesso controllato.	
<i>E' incaricato alla sorveglianza dei seguenti archivi di dati personali:</i>	<ul style="list-style-type: none"> • Faldoni su scaffali

Particolare importanza rivestirà l'attenzione che verrà dedicata alle procedure indicate nelle istruzioni per l'incaricato (Allegato 1, codice 7566.3.75202.284936) alle quali vi è l'obbligo di attenersi scrupolosamente. Vi è obbligo inoltre di prendere visione dei nominativi del personale autorizzato a trattare i dati relativi all'ambito a lei assegnato, siano essi titolare, responsabili o incaricati (Organigramma). Come incaricato è tenuto a prenderne visione ed a comunicare al responsabile eventuali inesattezze. Se il terminale o il Pc di lavoro consentisse la connessione con altre banche dati, il Suo incarico di trattamento comprenderà l'incarico di trattare anche i dati delle banche dati connesse, nei limiti in cui ciò sarà necessario all'efficiente e corretto svolgimento delle Sue mansioni e sempre in conformità al profilo di autorizzazione e alle possibilità e procedure indicate nelle istruzioni per l'incaricato (Allegato 1).

Si ribadisce per chiarezza che il presente incarico è strettamente collegato alle mansioni svolte da ciascun incaricato e necessario per lo svolgimento delle stesse e che, pertanto, non costituisce conferimento di nuova mansione o ruolo. L'incaricato dichiara di aver ricevuto, in Allegato 1, le istruzioni e si impegna, dopo averne presa visione, ad adottare tutte le misure necessarie alla loro attuazione. Dichiara, inoltre, di aver ricevuto, nell'Organigramma, l'elenco dei soggetti autorizzati al trattamento dei dati personali e di esserne quindi a conoscenza. L'incaricato del trattamento dovrà osservare scrupolosamente tutte le istruzioni ricevute e le misure di sicurezza già in atto, o che verranno comunicate in seguito dal titolare o dal responsabile del trattamento. La Sua firma del presente incarico costituisce consapevole accettazione degli obblighi assunti.

Per accettazione

ELVIO AROSIO



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

ISTRUZIONI PER L'INCARICATO

La legge definisce come incaricati "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".

Limitatamente all'ambito di competenza a lei assegnato nella Nomina dal Titolare o dal Responsabile, vengono sotto riportate le istruzioni a cui è tenuto ad attenersi nel trattamento di dati personali, in conformità alle normative vigenti sulla Privacy.

PROCEDURE PER LA CLASSIFICAZIONE DEI DATI.

L'incaricato deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge. Qualora non fosse in grado, deve fare riferimento al Responsabile o al Titolare del Trattamento.

La natura dei dati trattati

Vengono riportate di seguito le definizioni e i riferimenti normativi per una più chiara comprensione:

- dati personali: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- dati sensibili: la lettera d) del comma 1 dell'articolo 4 del codice definisce in tale modo i dati personali idonei a rivelare 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- dati giudiziari: tali sono considerati, dalla lettera e) del comma 1 dell'articolo 4 del codice, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u) del Dpr 313/2002, 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 sensi degli articoli 60 e 61 del codice di procedura penale;
- dati che presentano rischi specifici: tali dati sono considerati dall'articolo 17. Si tratta di dati che, pur non essendo così delicati come quelli sensibili e giudiziari, presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati, ovvero alle modalità di trattamento o agli effetti che esso può determinare: in considerazione di tale fatto, il loro trattamento è ammesso nel rispetto delle misure e degli accorgimenti, prescritti dal Garante a garanzia dei soggetti interessati.

AFFIDAMENTO AGLI INCARICATI DI DOCUMENTI, CONTENENTI DATI PERSONALI, E MODALITÀ DA OSSERVARE PER LA CUSTODIA DEGLI STESSI.

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare o del Responsabile in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare: non trattare nessun documento al di fuori delle autorizzazioni.

Una volta presi in carico, gli atti e i documenti, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma occorre provvedere in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni affidate.

In caso di affidamento di atti e documenti contenenti dati sensibili o giudiziari, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario dotarsi di cassette con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente (ad esempio, per recarsi in mensa). In mancanza di tali strumenti sollecitare la Direzione affinché provveda.

Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.

Qualora si debbano utilizzare anche nei giorni successivi i documenti potranno essere riposti in tali cassette al termine della giornata di lavoro. Al termine del trattamento dovranno invece essere restituiti all'archivio.

I SISTEMI INFORMATICI AZIENDALI

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto: tali strumenti vanno custoditi in modo appropriato e possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità aziendali. In questo contesto l'azienda potrà per necessità di sicurezza aziendale o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione.

Utilizzo del personal computer

- è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Titolare o dal Responsabile; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici; non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem);
- non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
- i Personal Computer "stand alone" o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Utilizzo di internet

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge;
- non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo definita 'sensibile' ai sensi del D.Lgs. 196/2003: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Titolare o dal Responsabile del Trattamento e con il rispetto delle normali procedure di acquisto;
- non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dal Titolare o dal Responsabile;
- non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non è permessa la partecipazione, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
- non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Utilizzo del servizio di posta elettronica

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente Riservati";
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list; solo in questo ultimo caso è possibile, previa autorizzazione per la verifica della validità dell'emittente, iscriversi a servizi di informazione strettamente inerenti all'attività aziendale;
- nel caso esista un dominio di proprietà aziendale (es.: nomeazienda.it) al quale sia collegato un servizio di posta e la relativa casella (es.: rossi@nomeazienda.it), non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai domini aziendali salvo diversa ed esplicita autorizzazione.

MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto.

Rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina ad Incaricato.

Nel caso in cui sia prevista la figura del custode delle copie credenziali, è necessario trascrivere una copia della propria parola chiave e consegnarla in busta chiusa (meglio se sigillata) all'incaricato od al responsabile addetto alla loro custodia. Fare riferimento al Titolare od al Responsabile per i dettagli operativi della procedura.

Elaborare le password seguendo le istruzioni sotto riportate.

SCelta DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

- NON dica a nessuno la sua password. Ricordi che lo scopo principale per cui usa una password è assicurare che nessun altro possa utilizzare le sue risorse o possa farlo a suo nome.
- NON scriva la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
- Quando immette la password NON faccia sbirciare a nessuno quello che sta battendo sulla tastiera.
- NON scelga password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- NON creda che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- NON usi il suo nome utente. È la password più semplice da indovinare.
- NON usi password che possano in qualche modo essere legate a lei come, ad esempio, il suo nome, quello di sua moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE OBBLIGATORIAMENTE

- la password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica;
- l'incaricato deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema;
- la password deve essere modificata dall'incaricato almeno ogni 6 mesi;
- se il trattamento riguarda dati sensibili o giudiziari la password deve essere modificata almeno ogni tre mesi ;

COSA FARE PRATICAMENTE

Utilizzare più di una parola e creare password lunghe

A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.

Inoltre è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un'ottima protezione contro possibili violazioni. Non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri: ad esempio i sistemi operativi Windows 95 98 e Me non oltrepassano questo limite.

Utilizzare numeri e simboli al posto di caratteri

Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:

- Caratteri minuscoli: a, b, c,...
- Caratteri maiuscoli: A, B, C,...
- Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
- Caratteri non alfanumerici: (< > , .) ` ~ ! \$ % ^ ; * - + = | \ { @ # } [/] : ; " ' ?

Non inserirli alla fine di una parola nota come ad es.: "computer987". In questo caso la password può essere identificata abbastanza facilmente: la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare. Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a utilizzare "@" al posto di "A", "\$" al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3" al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri. Con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve\$tit0 di Mari0"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare.

Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista.

OBBLIGO DI NON LASCIARE INCUSTODITI E ACCESSIBILI GLI STRUMENTI ELETTRONICI, MENTRE È IN CORSO UNA SESSIONE DI LAVORO.

Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. È necessario terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare, anche solo per cinque minuti effettuando un log out o mettendo in atto accorgimenti tali, per cui anche in quei cinque minuti il computer non resti:

- incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
- accessibile: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.

Non si devono invece mai verificare situazioni in cui lo strumento elettronico venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un incaricato al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave.

E' possibile installare strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato dall'utente in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previa imputazione di password. Verifichi con i Responsabili o con il Titolare le possibilità di abilitazione dello strumento.

PROCEDURE E MODALITÀ DI UTILIZZO DEGLI STRUMENTI E DEI PROGRAMMI ATTI A PROTEGGERE I SISTEMI INFORMATIVI.

In collaborazione con i Responsabili o con il Titolare, che possono installare dove previsti degli automatismi in grado di sostituirsi all'incaricato, prevedere di:

- aggiornare con cadenza almeno mensile gli antivirus installati sulla propria postazione PC. Si consigliano ovviamente cadenze più serrate;
- installare le Patch di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dati personali, con cadenza annuale che diviene semestrale in caso di trattamenti di dati sensibili o giudiziari.

FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

- riutilizzo di dischetti già adoperati in precedenza;
- uso di software gratuito (trial, freeware o shareware) prelevato da siti Internet o in allegato a riviste o libri;
- collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
- collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
- file attached di posta elettronica.

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come prevenire i virus:

1. Usi soltanto programmi provenienti da fonti fidate

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzi programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. Si assicuri che il suo software antivirus sia aggiornato

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Si informi attraverso il Portale della privacy sugli obblighi di legge in tema di aggiornamento degli antivirus e applichi, se possibile, una frequenza di aggiornamento mensile (più idonea di quella prevista dalla legge).

3. Si assicuri che il suo PC sia stato controllato dall'antivirus

Almeno una volta alla settimana e provveda a lanciare una scansione dell'intero sistema con il suo software antivirus. Se questo software lo prevede, scheduli anche in questo caso la programmazione della scansione in maniera tale da non doversi ricordare di lanciarla e lasciando che il programma la esegua in automatico. Si consulti con i Responsabili o con il Titolare per le informazioni necessarie.

4. Non diffonda messaggi di provenienza dubbia

Se riceve messaggi che avvisano di un nuovo virus pericolosissimo, lo ignori: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal suo migliore amico, dal suo capo o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).

5. Non partecipi a "catene di S. Antonio" o simili

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi

o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

6. Eviti la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete

7. Non utilizzi i server di rete come stazioni di lavoro

8. Non aggiunga mai dati o file ai floppy disk contenenti programmi originali

9. Si assicuri di non far partire accidentalmente il suo computer da dischetto.

Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

10. Protegga i suoi dischetti da scrittura quando possibile.

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

- Non si deve utilizzare il proprio floppy disk di sistema su di un altro computer se non in condizioni di protezione in scrittura;
- Se si utilizza un computer che necessita di essere avviato da floppy, usare un floppy disk protetto in scrittura;
- Non attivare mai da floppy un sistema basato su hard disk a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto;

OBBLIGO DI RISERVATEZZA E CAUTELA NELLA COMUNICAZIONE A TERZI DI DATI E INFORMAZIONI

Anche informazioni di normale quotidianità aziendale o ritenute non riservate all'interno dell'interscambio tra incaricati, assumono diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

SOCIAL ENGINEERING

Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurci ai propri scopi presentandosi personalmente presso di noi o contattandoci dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può anche renderci complici inconsapevoli di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene dialer o altro materiale pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi lanciare il virus, c'è un modo molto semplice: indurre la vittima, tramite espedienti psicologici a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo senso l'aggressore potrebbe essere capace di sfruttare i nostri punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

E-MAIL PHISHING

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Spesso queste tecniche sono abbinata tra loro e applicate più volte nel tempo sulla stessa vittima

COSA FARE

- non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- limitatevi a fornire informazioni a interlocutori noti e operanti con voi per disposizione aziendale, nei limiti dei contenuti afferenti all'ambito lavorativo a voi assegnato;
- diffidate di messaggi provenienti da fonte non conosciuta;
- non aprite messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprite messaggi contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il Responsabile o il Titolare.

PROCEDURE PER IL SALVATAGGIO DEI DATI.

Gli incaricati sono tenuti a fare riferimento alla politica interna di back up per le istruzioni specifiche di salvataggio. Se è nominato l'incaricato delle copie di back up, egli sarà il referente per tali operazioni.

CUSTODIA ED UTILIZZO DEI SUPPORTI RIMUOVIBILI, CONTENENTI DATI PERSONALI.

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. dischetti), contenenti dati sensibili o giudiziari, nei seguenti termini:

- I supporti rimovibili (es. dischetti), contenenti dati sensibili o giudiziari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassette chiuse a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
- Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

DOVERE DI AGGIORNARSI, UTILIZZANDO IL MATERIALE E GLI STRUMENTI FORNITI DALL'ORGANIZZAZIONE, SULLE MISURE DI SICUREZZA.

Pretendere dal titolare che vengano forniti strumenti per la formazione sulla privacy. In particolare relativamente a:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

ISTRUZIONI GENERICHE

L'INCARICATO DOVRA':

procedere alla raccolta di dati personali, nelle modalità previste dalle sue mansioni e indicate in apposita informativa;

consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa di cui all'art. 13 del nuovo Codice della Privacy, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;

raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il Titolare o il Responsabile, e salvo i casi di esonero previsti dalla stessa legge;

trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti, secondo quanto espresso nell'informativa e, comunque, in modo lecito e secondo correttezza;

adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate dal Titolare o dal Responsabile, in particolare dovrà:

- per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare rispettando strettamente il proprio profilo di autorizzazione;
- conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- copie di dati personali su supporti rimovibili sono permesse solo se parte del trattamento, copie di dati sensibili devono essere espressamente autorizzate dal Responsabile del trattamento o dal Titolare. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento o al Titolare;
- segnalare al Titolare o al Responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal Titolare o dal Responsabile e

- secondo le modalità stabilite dai medesimi e dichiarate nell'informativa;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
 - fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
 - in generale, prestare la più ampia e completa collaborazione al Titolare ed al Responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Manutenzione e gestione dei sistemi di elaborazione elettronica.

Tale area di competenza riguarda tutte le operazioni inerenti alla gestione e alla manutenzione del sistema informatico. Nel momento in cui i dati personali vengono trattati con l'ausilio di strumentazione informatica, la loro gestione deve essere conforme alle disposizioni di Legge in materia di sicurezza dei dati, come prescritto nel Codice della Privacy. In particolare Lei è tenuto a:

- Installare su tutte le postazioni client, sui server, sui PC e dove necessario (limitatamente all'ambito di competenza a lei assegnato) gli antivirus e aggiornarli con cadenza almeno semestrale! Si consiglia una frequenza del tutto più restrittiva.
- Effettuare tutti gli aggiornamenti patch dei sistemi operativi e dei programmi utilizzati per il trattamento dati, con cadenza annuale che diviene semestrale in caso di trattamenti di dati sensibili o giudiziari.
- Definire le politiche di protezione passiva della rete (firewall e sua configurazione) per la difesa del sistema dall'attacco di hackers.
- Verificare l'efficacia delle politiche di sicurezza almeno con cadenza semestrale.
- Collaborare con gli altri responsabili mantenendoli informati della gestione e di eventuali anomalie di sistema che potrebbero compromettere la sicurezza.
- Istruire gli incaricati dei back-up riguardo alle procedure da adottare per le operazioni di salvataggio delle copie di sicurezza dei dati personali, redigendo apposito documento di istruzioni. Risolvere gli eventuali problemi tecnici nella realizzazione dei back-up rilevati dai rispettivi incaricati.
- Sottoscrivere il documento con le istruzioni per il back up, conservarlo in luogo sicuro e trasmetterlo in copia agli incaricati del trattamento dei dati interessati alle copie di salvataggio, nonché all'incaricato dei back up di quella base dati. Per ogni base dati deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up e le modalità di custodia.
- Nel caso in cui la manutenzione venisse affidata ad una società esterna, è opportuno ricevere dalla stessa i nominativi delle persone che provvederanno alla manutenzione, al fine di redigere una lettera di incarico delle stesse; per tali operazioni fare riferimento al Titolare o al Responsabile dei trattamenti.

Back Up dei dati

Per back up si intende l'insieme di operazioni e di procedure mirate ad effettuare una copia di sicurezza dei dati personali memorizzati su dispositivi informatici, in modo da rendere possibile un eventuale ripristino dei dati nel caso si verificano eventi dannosi che portino al danneggiamento od alla perdita (totale o parziale) dei dati personali. In quanto incaricato della realizzazione dei Back-up in relazione alle banche dati di sua competenza, Lei è tenuto ad :

- Effettuare una copia dei dati personali almeno una volta alla settimana.
- Collaborare con l'Amministratore di Sistema o con il Responsabile dell'area sicurezza per la sequenza delle operazioni tecniche da effettuare.
- Segnalare in modo sollecito al relativo Responsabile o all'Amministratore di Sistema il presentarsi di eventuali problemi alla normale attività di copia delle basi di dati.
- Le copie di back-up devono essere custodite ed utilizzate in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.
- Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

Custodia delle Copie Credenziali

Il Codice della Privacy impone che siano studiate ed applicate procedure per consentire la continuità operativa dei trattamenti e quindi l'accesso ai computer anche nel caso in cui l'incaricato rimanesse a lungo assente o dimenticasse la propria password. Nell'ipotesi che i sistemi in uso non fossero in grado di permettere l'accesso di un altro soggetto con privilegi superiori (quello che in gergo tecnico viene chiamato "Admin", "Administrator" o "Amministratore") in grado di azzerare la precedente password per assegnarne una nuova e rendere disponibile nuovamente all'uso la postazione, una modalità comunemente adottata è quella di nominare un CUSTODE DELLE COPIE CREDENZIALI che conserva in un luogo sicuro e in busta chiusa copia di tutte le password in uso, per consultarle nel momento in cui si rendesse necessario accedere ad un elaboratore privo dell'incaricato o nel caso questi avesse smarrito la password.

In questi casi, è necessario:

- predisporre una copia della parola chiave, provvedendo quindi a trascriverla in copia, facendo però in modo che l'informazione resti segreta (ad esempio, inserendola in una busta chiusa e, possibilmente, sigillata);

- consegnare tale copia all'incaricato per la custodia delle copie credenziali o parole chiave;
- ripetere i due punti precedenti per ogni sostituzione periodica.

Verificare nell'Organigramma Privacy la presenza della figura del CUSTODE DELLE COPIE CREDENZIALI.

Sorveglianza degli Archivi ad Accesso Controllato

Tale area di competenza riguarda le operazioni di sorveglianza e controllo degli archivi contenenti dati sensibili o giudiziari. In particolare Lei è tenuto a:

- Assicurarsi che tali archivi siano situati in contenitori od uffici chiudibili a chiave.
- Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.
- Nel caso non vi siano apparecchiature elettroniche che identifichino e registrino gli accessi all'archivio od all'ufficio, tenere un registro manuale degli accessi fuori orario di lavoro. I soggetti che vengono ammessi agli archivi, dopo l'orario di chiusura degli stessi, devono essere identificati e registrati.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

ELENCO DEI TRATTAMENTI E DISTRIBUZIONE DEI COMPITI

Descrizione dei dati personali trattati, suddivisi per banche dati ed unità di archiviazione, ed organigramma della distribuzione dei compiti e delle responsabilità per il trattamento e la gestione dei dati.

La descrizione dettagliata delle aree di competenza, dei compiti e delle istruzioni affidati ai singoli soggetti è reperibile consultando la corrispondente nomina a responsabile od ad incaricato.

Titolare del trattamento : GAIN STUDIOS DI AROSIO ELVIO S.A.S. nella persona di ELVIO AROSIO

Responsabile al rapporto con gli interessati (art. 13) : ELVIO AROSIO

Sedi interessate ai trattamenti dei dati personali.

Sale Prove C/o Scuola Don Minzoni

<i>Indirizzo:</i>	Via Turati , 27100 Pavia (PV)
<i>Responsabili:</i>	<ul style="list-style-type: none"> Responsabile della sicurezza : ELVIO AROSIO Responsabile dei sistemi di elaborazione elettronica : ELVIO AROSIO
Sono sotto riportati gli uffici od i locali della sede interessati al trattamento od alla conservazione dei dati personali.	
<ul style="list-style-type: none"> Sala Attesa 	Sala di attesa con computer per la videosorveglianza

Sede Principale Azienda

<i>Indirizzo:</i>	Sede Principale azienda Viale Montegrappa 28/G , 27100 PAVIA (PV); e-mail: info@gainstudios.com; telefono: 0382 464161
<i>Responsabili:</i>	<ul style="list-style-type: none"> Responsabile della sicurezza : ELVIO AROSIO Responsabile dei sistemi di elaborazione elettronica : ELVIO AROSIO
Sono sotto riportati gli uffici od i locali della sede interessati al trattamento od alla conservazione dei dati personali.	
<ul style="list-style-type: none"> Ufficio Direzionale 	Ufficio al Primo Piano della sede principale

Banche Dati

Banca Dati : Acquisti

Dati anagrafici, Fatture, Ddt, Ordini, Preventivi, Documenti bancari, Rubriche, Corrispondenza

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> Codice fiscale ed altri numeri di identificazione personale Nominativo, indirizzo o altri elementi di identificazione personale Attività economiche, commerciali, finanziarie e assicurative
Unità di archiviazione della banca dati	
1 - Faldoni su scaffali (sede: Sede Principale azienda)	
<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati alla Sorveglianza</i>	<ul style="list-style-type: none"> ELVIO AROSIO

<i>degli archivi :</i>		
2 - Server (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
Banca Dati : Corsi e formazione		
Data anagrafici e di identificazione personale iscritti ai corsi, Registro presenze		
<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Istruzione e cultura 	
Unita' di archiviazione della banca dati		
1 - Faldoni su scaffali (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
2 - Server (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server	
<i>Ufficio:</i>	Ufficio Direzionale	
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione) 	
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO 	
Banca Dati : Curriculum		
Mail, Lettere, Fax.		
<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Lavoro • Istruzione e cultura • Abitudini di vita o di consumo • Voti, giudizi ed altri dati di valutazione del rendimento scolastico 	
<i>Dati Sensibili trattati :</i>	<ul style="list-style-type: none"> • Origini razziali o etniche • Convinzioni religiose • Convinzioni filosofiche o di altro genere • Opinioni politiche • Adesione a partiti • Adesione a sindacati • Stato di salute • Vita sessuale 	

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

2 - Server (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

Banca Dati : Gare e appalti

Capitolati, bandi, offerte, documenti di partecipazione, visure camerali con diciture antimafia

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Attività economiche, commerciali, finanziarie e assicurative • Istruzione e cultura • Beni, proprietà, possessi
<i>Dati Giudiziari trattati :</i>	<ul style="list-style-type: none"> • Informazioni concernenti i provvedimenti giudiziari

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

2 - Server (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

Banca Dati : Gestione Personale

Dati anagrafici, Contratti, Corrispondenza, Fogli presenze, Libro matricole, Cud e documenti obbligatori per legge

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Lavoro • Istruzione e cultura • Voti, giudizi ed altri dati di valutazione del rendimento scolastico • Dati relativi al tipo di lavoro ed alla retribuzione
<i>Dati Sensibili trattati :</i>	<ul style="list-style-type: none"> • Origini razziali o etniche • Convinzioni religiose • Opinioni politiche • Adesione a partiti • Adesione a sindacati • Stato di salute • Log File di Navigazione Internet

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

2 - Server (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati delle copie credenziali :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati ai back-up :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO
<i>Incaricati nominati amministratori del sistema informatico:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

Banca Dati : Marketing

Mail, Offerte, Fax, Rubriche

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative
-------------------------------	--

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati alla Sorveglianza degli archivi :</i>	<ul style="list-style-type: none"> • ELVIO AROSIO

2 - Server (sede: Sede Principale azienda)

<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
<i>Ufficio:</i>	Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>	<ul style="list-style-type: none"> • ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)

	<i>Incaricati delle copie credenziali :</i>	• ELVIO AROSIO
	<i>Incaricati ai back-up :</i>	• ELVIO AROSIO
	<i>Incaricati nominati amministratori del sistema informatico:</i>	• ELVIO AROSIO

Banca Dati : Posta elettronica

Mail, allegati, robriche

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Lavoro • Attività economiche, commerciali, finanziarie e assicurative • Istruzione e cultura • Beni, proprietà, possessi • Dati sul comportamento • Abitudini di vita o di consumo • Dati relativi allo svolgimento delle attività economiche dell'interessato. • Voti, giudizi ed altri dati di valutazione del rendimento scolastico • Dati relativi al tipo di lavoro ed alla retribuzione
<i>Dati Sensibili trattati :</i>	<ul style="list-style-type: none"> • Origini razziali o etniche • Convinzioni religiose • Convinzioni filosofiche o di altro genere • Opinioni politiche • Adesione a partiti • Adesione a sindacati • Stato di salute • Vita sessuale

Unita' di archiviazione della banca dati

1 - Server (sede: Sede Principale azienda)

	<i>Descrizione archivio:</i>	Server IBM con Microsoft Windows 2000 Server
	<i>Ufficio:</i>	Ufficio Direzionale
	<i>Incaricati al trattamento e permessi:</i>	• ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
	<i>Incaricati delle copie credenziali :</i>	• ELVIO AROSIO
	<i>Incaricati ai back-up :</i>	• ELVIO AROSIO
	<i>Incaricati nominati amministratori del sistema informatico:</i>	• ELVIO AROSIO

Banca Dati : Vendite

Dati anagrafici, Fatture, Ddt, Ordini, Preventivi, Documenti bancari, Rubriche, Corrispondenza, Rapporti di intervento (installazioni etc.)

<i>Dati Comuni trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative
-------------------------------	--

Unita' di archiviazione della banca dati

1 - Faldoni su scaffali (sede: Sede Principale azienda)

	<i>Descrizione archivio:</i>	Faldoni su scaffalatura a giorno in ferro e legno
	<i>Ufficio:</i>	Ufficio Direzionale
	<i>Incaricati al trattamento e permessi:</i>	• ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
	<i>Incaricati alla Sorveglianza degli archivi :</i>	• ELVIO AROSIO

2 - Server (sede: Sede Principale azienda)		
<i>Descrizione archivio:</i>		Server IBM con Microsoft Windows 2000 Server
<i>Ufficio:</i>		Ufficio Direzionale
<i>Incaricati al trattamento e permessi:</i>		• ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati delle copie credenziali :</i>		• ELVIO AROSIO
<i>Incaricati ai back-up :</i>		• ELVIO AROSIO
<i>Incaricati nominati amministratori del sistema informatico:</i>		• ELVIO AROSIO

Banca Dati : Videosorveglianza	
Filmati privi di audio.	
<i>Dati Sensibili trattati :</i>	• RegISTRAZIONI di videosorveglianza
Unita' di archiviazione della banca dati	

1 - Pc Videosorveglianza (sede: Sale prove C/o Scuola Don Minzoni)		
<i>Descrizione archivio:</i>		Prsonal Computer per Videosorveglianza
<i>Ufficio:</i>		Sala Attesa
<i>Incaricati al trattamento e permessi:</i>		• ELVIO AROSIO (permessi: lettura, scrittura, cancellazione, comunicazione)
<i>Incaricati delle copie credenziali :</i>		• ELVIO AROSIO
<i>Incaricati ai back-up :</i>		• ELVIO AROSIO
<i>Incaricati nominati amministratori del sistema informatico:</i>		• ELVIO AROSIO

Categorie di soggetti interessate al trattamento

Riportiamo ora in maggior dettaglio i trattamenti effettuati, distinguendo a quali soggetti interessati appartengono i dati oggetto di trattamento. Ulteriori informazioni a riguardo possono essere trovate, se previste, nelle relative informative.

Categoria di soggetti interessata : Candidati da considerare per l'instaurazione di un rapporto di lavoro	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Curriculum • Posta elettronica
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Abitudini di vita o di consumo • Adesione a partiti • Adesione a sindacati • Codice fiscale ed altri numeri di identificazione personale • Convinzioni filosofiche o di altro genere • Convinzioni religiose • Dati relativi alla famiglia e a situazioni personali • Istruzione e cultura • Lavoro • Nominativo, indirizzo o altri elementi di identificazione personale • Opinioni politiche • Origini razziali o etniche • Stato di salute • Vita sessuale • Voti, giudizi ed altri dati di valutazione del rendimento scolastico
<i>Finalità del trattamento :</i>	• Selezione del personale per l'instaurazione di un rapporto di lavoro
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei

Categoria di soggetti interessata : Clienti	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Vendite • Posta elettronica • Marketing
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Eventualmente per soddisfare indagini di mercato, statistiche e per attività promozionali inerenti anche alla spedizione di materiale pubblicitario e promozionale • Adempimenti obbligatori per legge in campo fiscale e contabile • Assistenza post-vendita • Gestione del contenzioso • Gestione della clientela • Gestione della Qualità • Programmazione delle attività • Rilevazione del grado di soddisfazione della clientela • Storico fatturazione clienti
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Affidamento a terzi di operazioni di elaborazione • Creazione di profili relativi a clienti, fornitori o consumatori • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Consulenti e liberi professionisti, anche in forma associata • Banche e istituti di credito • Spedizionieri, Trasportatori, Padroncini, Poste, Aziende per la Logistica
Categoria di soggetti interessata : Potenziali clienti	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Posta elettronica • Marketing
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Eventualmente per soddisfare indagini di mercato, statistiche e per attività promozionali inerenti anche alla spedizione di materiale pubblicitario e promozionale
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Elaborazione di dati raccolti da terzi • Raccolta di dati in luoghi pubblici o aperti al pubblico. • Raccolta di dati tramite schede, coupons e questionari. • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
Categoria di soggetti interessata : Fornitori	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Acquisti • Posta elettronica
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Adempimenti obbligatori per legge in campo fiscale e contabile • Gestione dei fornitori • Gestione del contenzioso • Gestione della Qualità • Di obblighi previsti dalle leggi vigenti • Programmazione delle attività • Storico ordini forniture
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Affidamento a terzi di operazioni di elaborazione • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Consulenti e liberi professionisti, anche in forma associata • Banche e istituti di credito • Nell'ambito di soggetti pubblici e/o privati per i quali la comunicazione dei dati è obbligatoria o necessaria in adempimento ad obblighi di legge o sia comunque

	<p>funzionale all'amministrazione del rapporto</p> <ul style="list-style-type: none"> • Spedizionieri, Trasportatori, Padroncini, Poste, Aziende per la Logistica
Categoria di soggetti interessata : Dipendenti e personale parasubordinato	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Gestione Personale
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Adesione a partiti • Adesione a sindacati • Codice fiscale ed altri numeri di identificazione personale • Convinzioni religiose • Dati relativi al tipo di lavoro ed alla retribuzione • Dati relativi alla famiglia e a situazioni personali • Istruzione e cultura • Lavoro • Log File di Navigazione Internet • Nominativo, indirizzo o altri elementi di identificazione personale • Opinioni politiche • Origini razziali o etniche • Stato di salute • Voti, giudizi ed altri dati di valutazione del rendimento scolastico
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali • Adempimenti obbligatori per legge in campo fiscale e contabile • Gestione del contenzioso • Gestione del personale in genere • Gestione della Qualità • Igiene e sicurezza del lavoro • Programmazione delle attività • Servizi di controllo interno • Trattamento giuridico ed economico del personale
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Affidamento a terzi di operazioni di elaborazione • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Organi costituzionali o di rilievo costituzionale • Enti previdenziali e assistenziali • Organizzazioni sindacali e patronati • Consulenti e liberi professionisti, anche in forma associata • Banche e istituti di credito • Imprese di assicurazione • Familiari dell'interessato
Categoria di soggetti interessata : Interessati Videosorveglianza	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Videosorveglianza
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • RegISTRAZIONI di videosorveglianza
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Servizio di controllo/sicurezza e Conservazione registrazioni per 24 ore
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Forze di polizia
Categoria di soggetti interessata : Corsisti	
<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Marketing • Corsi e formazione
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Codice fiscale ed altri numeri di identificazione personale • Istruzione e cultura • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Stesura relazione a committente

	<ul style="list-style-type: none"> • Compilazione attestati di frequenza • Gestione esercitazioni pratiche • Pianificazione attività dei corsi
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Committenti • Familiari dell'interessato • Subfornitori

Categoria di soggetti interessata : Socio e Società

<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Gare e appalti
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Attività economiche, commerciali, finanziarie e assicurative • Beni, proprietà, possessi • Codice fiscale ed altri numeri di identificazione personale • Dati relativi alla famiglia e a situazioni personali • Informazioni concernenti i provvedimenti giudiziari • Istruzione e cultura • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Presentazione di offerte per partecipazione a gare ed appalti
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei
<i>I dati sopra riportati potranno essere comunicati a :</i>	<ul style="list-style-type: none"> • Committenti

Categoria di soggetti interessata : Committenza

<i>Banche dati coinvolte :</i>	<ul style="list-style-type: none"> • Gare e appalti
<i>Dati trattati :</i>	<ul style="list-style-type: none"> • Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
<i>Finalità del trattamento :</i>	<ul style="list-style-type: none"> • Presentazione di offerte per partecipazione a gare ed appalti
<i>Tipologie di trattamento dei dati :</i>	<ul style="list-style-type: none"> • Trattamento a mezzo di calcolatori elettronici • Trattamento manuale a mezzo di archivi cartacei



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

Il Titolare

Titolare : GAIN STUDIOS DI AROSIO ELVIO S.A.S. nella persona di ELVIO AROSIO

La Legge definisce come titolare la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Al titolare spettano, per presunzione assoluta di legge, la direzione delle attività di trattamento dei dati personali: a tale soggetto competono infatti le decisioni strategiche di fondo su come (modalità) e perché (finalità) raccogliere e trattare i dati, nonché sull'organizzazione del trattamento e sulle risorse (strumenti) da dedicarvi, anche per garantire la sicurezza. Il titolare si identifica con la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo cui oggettivamente spettano tali decisioni di fondo.

Nel caso di persone giuridiche, tale figura tende in generale a coincidere con il legale rappresentante della società o dell'ente potendosi così individuare, anche nell'ambito di strutture complesse, chi sia specificamente: tale soggetto sarà sempre e comunque tenuto in prima persona a rispondere per i danni cagionati nel trattamento dei dati, nonché delle sanzioni di carattere civilistico ed amministrativo.

E' inoltre possibile che, da parte delle autorità preposte all'accertamento degli eventuali reati, le responsabilità di ordine penale vengano estese a tutti i componenti dell'organo cui spetta la direzione della società e dell'ente (ad esempio, i membri del Consiglio di Amministrazione).

Compiti del Titolare

E' compito del titolare:

- Mettere in atto e verificare l'applicazione di tutte le disposizioni di legge in ordine ai trattamenti di dati personali in corso.
- Adottare e verificare l'implementazione delle misure di sicurezza previste dal Codice della Privacy per garantire l'idonea protezione ai dati, ponendo particolare attenzione alle misure minime di sicurezza.
- Individuare e nominare gli incaricati ai trattamenti di dati personali, per iscritto e fornendo loro istruzioni per poter operare in modo corretto e secondo quanto disposto dal Codice della Privacy anche in riferimento alle misure di sicurezza.
- Eventualmente individuare e nominare dei responsabili tramite lettera di nomina scritta definendo le aree di competenza (trattamento dei dati, sicurezza, gestione dei sistemi di elaborazione elettronica, rapporto con gli interessati) e i compiti assegnati.
- Provvedere a fornire a Responsabili e Incaricati l'adeguata istruzione riguardo le disposizioni di legge contenute nel Codice della Privacy che regolano le responsabilità, le funzioni e gli scopi propri della loro mansione nonché le norme basilari relative ai trattamenti e alla protezione dei dati.
- Il Titolare del trattamento può ritenere di non nominare alcun responsabile con la consapevolezza di accollarsi per intero le responsabilità e le funzioni loro proprie. In questo caso sarà sua preoccupazione realizzare l'intero adeguamento di Legge secondo tutte le norme e le disposizioni in essa contenute.

In particolare, non essendo stati nominati dei Responsabili in tutte le aree di competenza, sono sotto riportati , divisi per aree di competenza, i compiti che devono essere eseguiti dal titolare, almeno fino alla nomina dei relativi Responsabili.

Trattamento dei dati

L'area 'trattamento dati' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni inerenti alla gestione dei rapporti tra il Titolare e il Garante, tra il Titolare e gli interessati, e alla gestione operativa dei trattamenti dei dati personali:

- gestione notifica
- gestione rapporti con il Garante
- verifica corrispondenza con Autorizzazioni Annuali

- gestione comunicazione e diffusione dei dati secondo legge
- gestione informativa e consenso verso interessati
- gestione diritti di accesso degli interessati
- gestione delle modalità dei trattamenti interni
- nomina degli incaricati del trattamento
- creazione e gestione dei profili di autorizzazione
- gestione dei trattamenti affidati a terzi
- gestione della formazione da impartire agli incaricati

Individuare e nominare Incaricati dei trattamenti tutti coloro che sono addetti al trattamento esecutivo dei dati personali.

È compito del Responsabile ai Trattamenti:

- Raggiungere un sufficiente grado di apprendimento in materia di Privacy in modo da poter trattare i dati secondo la Legge e realmente vigilare sulla liceità e sulla correttezza dei trattamenti.
- Predisporre la notificazione iniziale al Garante nel caso in cui il trattamento rientri nei casi contemplati dall'art.37 del Codice, attraverso il programma Web disponibile sul sito del Garante (www.garanteprivacy.it), verificando l'esattezza e la completezza dei dati contenuti.
- Interagire con il Garante, in caso di richieste di informazioni o effettuazione di controlli ed accessi da parte dell'autorità;
- Censire analiticamente le banche dati con tutti gli elementi necessari per la determinazione dei trattamenti e delle tipologie di dati da inserire nel DPSS (dati trattati, tipi di trattamento, categorie di interessati, sedi e uffici del trattamento e in collaborazione con il Responsabile della Sicurezza, l'elenco dei sistemi di elaborazione nei quali avvengono i trattamenti), anche ai fini della eventuale notifica al Garante;
- Verificare che i trattamenti dei dati sensibili rientrino nelle Autorizzazioni del Garante in corso di validità ed, eventualmente, predisporre la richiesta di autorizzazione preventiva al trattamento di dati sensibili nel caso in cui il trattamento non rientri in tali Autorizzazioni.
- Procedere alla gestione delle informative e delle richieste di consenso nei casi e nelle modalità previste dalla legge
- Gestire il diritto di accesso degli interessati, agendo prontamente per soddisfare le loro richieste secondo l'art. 7; a questo proposito il Responsabile del trattamento ha la facoltà di nominare un Responsabile del Diritto di Accesso, al quale può delegare tale compito.
- Aggiornare l'elenco dei trattamenti in relazione ad eventuali nuovi trattamenti di dati personali;
- Individuare e nominare gli incaricati del trattamento impartendo loro, per iscritto, la nomina, le istruzioni e le autorizzazioni necessarie ad un corretto, lecito e sicuro trattamento, verificandone la puntuale applicazione;
- Produrre le nomine, le istruzioni e la distribuzione dei compiti (mansionario privacy) da consegnare ai medesimi per la firma e l'archiviazione.
- Collaborare con eventuali altri Responsabili e con l'eventuale Amministratore di Sistema.
- Definire i profili di autorizzazione (ambiti di competenza e operazioni consentite) degli incaricati
- Autorizzare i singoli incaricati al trattamento specifico di dati sensibili e giudiziari ponendo bene in evidenza tale fatto nella definizione del profilo di autorizzazione;
- Tenere aggiornato l'elenco dei trattamenti (censimento delle banche dati, tipologie di dati trattati, sedi in cui vengono trattati) e la distribuzione dei compiti (mansionario della privacy), con cadenza almeno annuale.
- Periodicamente con cadenza almeno annuale verificare la correttezza dei profili di autorizzazione revisionando gli ambiti di competenza ed eventualmente adattandoli a nuove esigenze.
- Provvedere a eliminare le autorizzazioni che rimangono inutilizzate oltre i sei mesi, sempre che il profilo particolare non determini per propria definizione un trattamento sporadico.
- Attuare gli obblighi di informazione ad acquisizione del consenso, quando richiesto, nei confronti degli interessati; delegare eventualmente questa incombenza ai singoli incaricati. A tal fine è possibile utilizzare i moduli e le procedure predisposte attraverso il Portale della Privacy.
- Individuare i trattamenti che vengono ceduti a Terzi (ad es. la gestione delle paghe) e attuare i necessari provvedimenti affinché tali trattamenti avvengano secondo liceità e correttezza garantendo lo standard di sicurezza previsto dalla legge. Il Responsabile deve decidere se nominare Responsabile la società terza in oggetto, se nominare Incaricati i soggetti individuali terzi che materialmente effettueranno i trattamenti o se introdurre restrittive clausole di garanzia nel contratto di fornitura del servizio. In queste operazioni può collaborare con l'eventuale Responsabile dell'area sicurezza.
- Verificare che tutti i trattamenti avvengano nel rispetto delle disposizioni di legge.
- Distruggere i dati personali che non sono più oggetto di trattamento alcuno.
- Informare prontamente il Titolare ed il personale interno addetto alla privacy di ogni questione rilevante ai fini di legge;
- Comunicare al Titolare qualsiasi elemento oggettivo o soggettivo che possa compromettere il corretto trattamento dei dati personali.
- Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del Titolare; nel caso venga delegato il trattamento all'esterno gestire il trattamento tramite terzi attuando le misure necessarie affinché sia garantita la sicurezza dei dati esportati, questo anche in collaborazione con l'eventuale Responsabile dell'area sicurezza.
- Collaborare con l'eventuale Responsabile dell'area sicurezza e con l'eventuale Amministratore di Sistema nella definizione delle credenziali di autenticazione e dei profili di autorizzazione.
- Elaborare un piano di formazione per rendere edotti gli incaricati del trattamento delle disposizioni di legge sulle modalità e i criteri del trattamento, nonché dei rischi individuati e dei modi per prevenire danni, anche in collaborazione con gli altri Responsabili.
- Collaborare con tutti i responsabili per l'attuazione delle prescrizioni impartite dal Garante attraverso nuove circolari,

- autorizzazioni e aggiornamenti di Legge;
- Gestire la cifratura e la separazione nei casi in cui vi sia la coesistenza di dati identificativi dell'interessato e dati sensibili, con particolare riferimento a quelli sanitari, che consentano una immediata associazione tra di essi. E' possibile fare riferimento alle soluzioni proposte dal Portale della Privacy.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

ISTRUZIONI PER L'INCARICATO

La legge definisce come incaricati "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".

Limitatamente all'ambito di competenza a lei assegnato nella Nomina dal Titolare o dal Responsabile, vengono sotto riportate le istruzioni a cui è tenuto ad attenersi nel trattamento di dati personali, in conformità alle normative vigenti sulla Privacy.

PROCEDURE PER LA CLASSIFICAZIONE DEI DATI.

L'incaricato deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge. Qualora non fosse in grado, deve fare riferimento al Responsabile o al Titolare del Trattamento.

La natura dei dati trattati

Vengono riportate di seguito le definizioni e i riferimenti normativi per una più chiara comprensione:

- dati personali: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- dati sensibili: la lettera d) del comma 1 dell'articolo 4 del codice definisce in tale modo i dati personali idonei a rivelare 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- dati giudiziari: tali sono considerati, dalla lettera e) del comma 1 dell'articolo 4 del codice, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u) del Dpr 313/2002, 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 sensi degli articoli 60 e 61 del codice di procedura penale;
- dati che presentano rischi specifici: tali dati sono considerati dall'articolo 17. Si tratta di dati che, pur non essendo così delicati come quelli sensibili e giudiziari, presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati, ovvero alle modalità di trattamento o agli effetti che esso può determinare: in considerazione di tale fatto, il loro trattamento è ammesso nel rispetto delle misure e degli accorgimenti, prescritti dal Garante a garanzia dei soggetti interessati.

AFFIDAMENTO AGLI INCARICATI DI DOCUMENTI, CONTENENTI DATI PERSONALI, E MODALITÀ DA OSSERVARE PER LA CUSTODIA DEGLI STESSI.

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare o del Responsabile in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare: non trattare nessun documento al di fuori delle autorizzazioni.

Una volta presi in carico, gli atti e i documenti, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma occorre provvedere in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni affidate.

In caso di affidamento di atti e documenti contenenti dati sensibili o giudiziari, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario dotarsi di cassette con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente (ad esempio, per recarsi in mensa). In mancanza di tali strumenti sollecitare la Direzione affinché provveda.

Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.

Qualora si debbano utilizzare anche nei giorni successivi i documenti potranno essere riposti in tali cassette al termine della giornata di lavoro. Al termine del trattamento dovranno invece essere restituiti all'archivio.

I SISTEMI INFORMATICI AZIENDALI

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto: tali strumenti vanno custoditi in modo appropriato e possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità aziendali. In questo contesto l'azienda potrà per necessità di sicurezza aziendale o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione.

Utilizzo del personal computer

- è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Titolare o dal Responsabile; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici; non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem);
- non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
- i Personal Computer "stand alone" o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Utilizzo di internet

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge;
- non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo definita 'sensibile' ai sensi del D.Lgs. 196/2003: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Titolare o dal Responsabile del Trattamento e con il rispetto delle normali procedure di acquisto;
- non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dal Titolare o dal Responsabile;
- non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non è permessa la partecipazione, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
- non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Utilizzo del servizio di posta elettronica

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente Riservati";
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list; solo in questo ultimo caso è possibile, previa autorizzazione per la verifica della validità dell'emittente, iscriversi a servizi di informazione strettamente inerenti all'attività aziendale;
- nel caso esista un dominio di proprietà aziendale (es.: nomeazienda.it) al quale sia collegato un servizio di posta e la relativa casella (es.: rossi@nomeazienda.it), non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai domini aziendali salvo diversa ed esplicita autorizzazione.

MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto.

Rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina ad Incaricato.

Nel caso in cui sia prevista la figura del custode delle copie credenziali, è necessario trascrivere una copia della propria parola chiave e consegnarla in busta chiusa (meglio se sigillata) all'incaricato od al responsabile addetto alla loro custodia. Fare riferimento al Titolare od al Responsabile per i dettagli operativi della procedura.

Elaborare le password seguendo le istruzioni sotto riportate.

SCelta DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

- NON dica a nessuno la sua password. Ricordi che lo scopo principale per cui usa una password è assicurare che nessun altro possa utilizzare le sue risorse o possa farlo a suo nome.
- NON scriva la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
- Quando immette la password NON faccia sbirciare a nessuno quello che sta battendo sulla tastiera.
- NON scelga password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- NON creda che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- NON usi il suo nome utente. È la password più semplice da indovinare.
- NON usi password che possano in qualche modo essere legate a lei come, ad esempio, il suo nome, quello di sua moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE OBBLIGATORIAMENTE

- la password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica;
- l'incaricato deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema;
- la password deve essere modificata dall'incaricato almeno ogni 6 mesi;
- se il trattamento riguarda dati sensibili o giudiziari la password deve essere modificata almeno ogni tre mesi ;

COSA FARE PRATICAMENTE

Utilizzare più di una parola e creare password lunghe

A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.

Inoltre è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un'ottima protezione contro possibili violazioni. Non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri: ad esempio i sistemi operativi Windows 95 98 e Me non oltrepassano questo limite.

Utilizzare numeri e simboli al posto di caratteri

Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:

- Caratteri minuscoli: a, b, c,...
- Caratteri maiuscoli: A, B, C,...
- Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
- Caratteri non alfanumerici: (< > , .) ` ~ ! \$ % ^ ; * - + = | \ { @ # } [/] : ; " ' ?

Non inserirli alla fine di una parola nota come ad es.: "computer987". In questo caso la password può essere identificata abbastanza facilmente: la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare. Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a utilizzare "@" al posto di "A", "\$" al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3" al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri. Con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve\$tit0 di Mari0"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare.

Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista.

OBBLIGO DI NON LASCIARE INCUSTODITI E ACCESSIBILI GLI STRUMENTI ELETTRONICI, MENTRE È IN CORSO UNA SESSIONE DI LAVORO.

Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. È necessario terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare, anche solo per cinque minuti effettuando un log out o mettendo in atto accorgimenti tali, per cui anche in quei cinque minuti il computer non resti:

- incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
- accessibile: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.

Non si devono invece mai verificare situazioni in cui lo strumento elettronico venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un incaricato al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave.

E' possibile installare strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato dall'utente in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previa imputazione di password. Verifichi con i Responsabili o con il Titolare le possibilità di abilitazione dello strumento.

PROCEDURE E MODALITÀ DI UTILIZZO DEGLI STRUMENTI E DEI PROGRAMMI ATTI A PROTEGGERE I SISTEMI INFORMATIVI.

In collaborazione con i Responsabili o con il Titolare, che possono installare dove previsti degli automatismi in grado di sostituirsi all'incaricato, prevedere di:

- aggiornare con cadenza almeno mensile gli antivirus installati sulla propria postazione PC. Si consigliano ovviamente cadenze più serrate;
- installare le Patch di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dati personali, con cadenza annuale che diviene semestrale in caso di trattamenti di dati sensibili o giudiziari.

FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

- riutilizzo di dischetti già adoperati in precedenza;
- uso di software gratuito (trial, freeware o shareware) prelevato da siti Internet o in allegato a riviste o libri;
- collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
- collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
- file attached di posta elettronica.

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come prevenire i virus:

1. Usi soltanto programmi provenienti da fonti fidate

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzi programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. Si assicuri che il suo software antivirus sia aggiornato

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Si informi attraverso il Portale della privacy sugli obblighi di legge in tema di aggiornamento degli antivirus e applichi, se possibile, una frequenza di aggiornamento mensile (più idonea di quella prevista dalla legge).

3. Si assicuri che il suo PC sia stato controllato dall'antivirus

Almeno una volta alla settimana e provveda a lanciare una scansione dell'intero sistema con il suo software antivirus. Se questo software lo prevede, scheduli anche in questo caso la programmazione della scansione in maniera tale da non doversi ricordare di lanciarla e lasciando che il programma la esegua in automatico. Si consulti con i Responsabili o con il Titolare per le informazioni necessarie.

4. Non diffonda messaggi di provenienza dubbia

Se riceve messaggi che avvisano di un nuovo virus pericolosissimo, lo ignori: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal suo migliore amico, dal suo capo o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).

5. Non partecipi a "catene di S. Antonio" o simili

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi

o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

6. Eviti la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete

7. Non utilizzi i server di rete come stazioni di lavoro

8. Non aggiunga mai dati o file ai floppy disk contenenti programmi originali

9. Si assicuri di non far partire accidentalmente il suo computer da dischetto.

Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

10. Protegga i suoi dischetti da scrittura quando possibile.

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

- Non si deve utilizzare il proprio floppy disk di sistema su di un altro computer se non in condizioni di protezione in scrittura;
- Se si utilizza un computer che necessita di essere avviato da floppy, usare un floppy disk protetto in scrittura;
- Non attivare mai da floppy un sistema basato su hard disk a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto;

OBBLIGO DI RISERVATEZZA E CAUTELA NELLA COMUNICAZIONE A TERZI DI DATI E INFORMAZIONI

Anche informazioni di normale quotidianità aziendale o ritenute non riservate all'interno dell'interscambio tra incaricati, assumono diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

SOCIAL ENGINEERING

Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurci ai propri scopi presentandosi personalmente presso di noi o contattandoci dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può anche renderci complici inconsapevoli di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene dialer o altro materiale pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi lanciare il virus, c'è un modo molto semplice: indurre la vittima, tramite espedienti psicologici a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo senso l'aggressore potrebbe essere capace di sfruttare i nostri punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

E-MAIL PHISHING

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Spesso queste tecniche sono abbinata tra loro e applicate più volte nel tempo sulla stessa vittima

COSA FARE

- non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- limitatevi a fornire informazioni a interlocutori noti e operanti con voi per disposizione aziendale, nei limiti dei contenuti afferenti all'ambito lavorativo a voi assegnato;
- diffidate di messaggi provenienti da fonte non conosciuta;
- non aprite messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprite messaggi contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il Responsabile o il Titolare.

PROCEDURE PER IL SALVATAGGIO DEI DATI.

Gli incaricati sono tenuti a fare riferimento alla politica interna di back up per le istruzioni specifiche di salvataggio. Se è nominato l'incaricato delle copie di back up, egli sarà il referente per tali operazioni.

CUSTODIA ED UTILIZZO DEI SUPPORTI RIMUOVIBILI, CONTENENTI DATI PERSONALI.

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. dischetti), contenenti dati sensibili o giudiziari, nei seguenti termini:

- I supporti rimovibili (es. dischetti), contenenti dati sensibili o giudiziari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassette chiuse a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
- Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

DOVERE DI AGGIORNARSI, UTILIZZANDO IL MATERIALE E GLI STRUMENTI FORNITI DALL'ORGANIZZAZIONE, SULLE MISURE DI SICUREZZA.

Pretendere dal titolare che vengano forniti strumenti per la formazione sulla privacy. In particolare relativamente a:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

ISTRUZIONI GENERICHE

L'INCARICATO DOVRA':

procedere alla raccolta di dati personali, nelle modalità previste dalle sue mansioni e indicate in apposita informativa;

consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa di cui all'art. 13 del nuovo Codice della Privacy, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;

raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il Titolare o il Responsabile, e salvo i casi di esonero previsti dalla stessa legge;

trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti, secondo quanto espresso nell'informativa e, comunque, in modo lecito e secondo correttezza;

adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate dal Titolare o dal Responsabile, in particolare dovrà:

- per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare rispettando strettamente il proprio profilo di autorizzazione;
- conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- copie di dati personali su supporti rimovibili sono permesse solo se parte del trattamento, copie di dati sensibili devono essere espressamente autorizzate dal Responsabile del trattamento o dal Titolare. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento o al Titolare;
- segnalare al Titolare o al Responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal Titolare o dal Responsabile e

- secondo le modalità stabilite dai medesimi e dichiarate nell'informativa;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
 - fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
 - in generale, prestare la più ampia e completa collaborazione al Titolare ed al Responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Manutenzione e gestione dei sistemi di elaborazione elettronica.

Tale area di competenza riguarda tutte le operazioni inerenti alla gestione e alla manutenzione del sistema informatico. Nel momento in cui i dati personali vengono trattati con l'ausilio di strumentazione informatica, la loro gestione deve essere conforme alle disposizioni di Legge in materia di sicurezza dei dati, come prescritto nel Codice della Privacy. In particolare Lei è tenuto a:

- Installare su tutte le postazioni client, sui server, sui PC e dove necessario (limitatamente all'ambito di competenza a lei assegnato) gli antivirus e aggiornarli con cadenza almeno semestrale! Si consiglia una frequenza del tutto più restrittiva.
- Effettuare tutti gli aggiornamenti patch dei sistemi operativi e dei programmi utilizzati per il trattamento dati, con cadenza annuale che diviene semestrale in caso di trattamenti di dati sensibili o giudiziari.
- Definire le politiche di protezione passiva della rete (firewall e sua configurazione) per la difesa del sistema dall'attacco di hackers.
- Verificare l'efficacia delle politiche di sicurezza almeno con cadenza semestrale.
- Collaborare con gli altri responsabili mantenendoli informati della gestione e di eventuali anomalie di sistema che potrebbero compromettere la sicurezza.
- Istruire gli incaricati dei back-up riguardo alle procedure da adottare per le operazioni di salvataggio delle copie di sicurezza dei dati personali, redigendo apposito documento di istruzioni. Risolvere gli eventuali problemi tecnici nella realizzazione dei back-up rilevati dai rispettivi incaricati.
- Sottoscrivere il documento con le istruzioni per il back up, conservarlo in luogo sicuro e trasmetterlo in copia agli incaricati del trattamento dei dati interessati alle copie di salvataggio, nonché all'incaricato dei back up di quella base dati. Per ogni base dati deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up e le modalità di custodia.
- Nel caso in cui la manutenzione venisse affidata ad una società esterna, è opportuno ricevere dalla stessa i nominativi delle persone che provvederanno alla manutenzione, al fine di redigere una lettera di incarico delle stesse; per tali operazioni fare riferimento al Titolare o al Responsabile dei trattamenti.

Back Up dei dati

Per back up si intende l'insieme di operazioni e di procedure mirate ad effettuare una copia di sicurezza dei dati personali memorizzati su dispositivi informatici, in modo da rendere possibile un eventuale ripristino dei dati nel caso si verificano eventi dannosi che portino al danneggiamento od alla perdita (totale o parziale) dei dati personali. In quanto incaricato della realizzazione dei Back-up in relazione alle banche dati di sua competenza, Lei è tenuto ad :

- Effettuare una copia dei dati personali almeno una volta alla settimana.
- Collaborare con l'Amministratore di Sistema o con il Responsabile dell'area sicurezza per la sequenza delle operazioni tecniche da effettuare.
- Segnalare in modo sollecito al relativo Responsabile o all'Amministratore di Sistema il presentarsi di eventuali problemi alla normale attività di copia delle basi di dati.
- Le copie di back-up devono essere custodite ed utilizzate in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.
- Particolare attenzione va riservata alle copie di back-up contenenti dati sensibili o giudiziari: è bene conservare gli archivi di back-up in cassette chiuse a chiave, durante il periodo di conservazione, e successivamente formattarli quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
- Nel caso di perdita di dati sensibili o giudiziari il ripristino delle copie di back-up deve essere effettuato in modo da consentire la ripresa a pieno regime entro e non oltre una settimana di tempo. A tale scopo, l'incaricato deve rifarsi al piano di continuità elaborato dal titolare o dal responsabile al trattamento.
- Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

Custodia delle Copie Credenziali

Il Codice della Privacy impone che siano studiate ed applicate procedure per consentire la continuità operativa dei trattamenti e quindi l'accesso ai computer anche nel caso in cui l'incaricato rimanesse a lungo assente o dimenticasse la propria password. Nell'ipotesi che i sistemi in uso non fossero in grado di permettere l'accesso di un altro soggetto con privilegi superiori (quello che in gergo tecnico viene chiamato "Admin", "Administrator" o "Amministratore") in grado di azzerare la precedente password per assegnarne una nuova e rendere disponibile nuovamente all'uso la postazione, una modalità comunemente adottata è

quella di nominare un CUSTODE DELLE COPIE CREDENZIALI che conserva in un luogo sicuro e in busta chiusa copia di tutte le password in uso, per consultarle nel momento in cui si rendesse necessario accedere ad un elaboratore privo dell'incaricato o nel caso questi avesse smarrito la password.

In questi casi, è necessario:

- predisporre una copia della parola chiave, provvedendo quindi a trascriverla in copia, facendo però in modo che l'informazione resti segreta (ad esempio, inserendola in una busta chiusa e, possibilmente, sigillata);
- consegnare tale copia all'incaricato per la custodia delle copie credenziali o parole chiave;
- ripetere i due punti precedenti per ogni sostituzione periodica.

Verificare nell'Organigramma Privacy la presenza della figura del CUSTODE DELLE COPIE CREDENZIALI.

Sorveglianza degli Archivi ad Accesso Controllato

Tale area di competenza riguarda le operazioni di sorveglianza e controllo degli archivi contenenti dati sensibili o giudiziari. In particolare Lei è tenuto a:

- Assicurarsi che tali archivi siano situati in contenitori od uffici chiudibili a chiave.
- Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.
- Nel caso non vi siano apparecchiature elettroniche che identifichino e registrino gli accessi all'archivio od all'ufficio, tenere un registro manuale degli accessi fuori orario di lavoro. I soggetti che vengono ammessi agli archivi, dopo l'orario di chiusura degli stessi, devono essere identificati e registrati.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

Atto di Nomina del Responsabile

GAIN STUDIOS DI AROSIO ELVIO S.A.S. nella persona di ELVIO AROSIO in qualità di 'Titolare del Trattamento' dei dati personali, ai sensi e per gli effetti del art. 29 del D.Lgs 30 Giugno 2003 n. 196 con il presente atto NOMINA :

Il Sig./Sig.ra ELVIO AROSIO

RESPONSABILE del trattamento dei dati personali per le aree di competenza di seguito definite:

Area 'rapporto con gli interessati'.

E' responsabile del rapporto con i soggetti a cui appartengono i dati personali

Area 'sicurezza' dei dati personali.

E' responsabile alla sicurezza per le seguenti sedi:

- Sale prove C/o Scuola Don Minzoni
- Sede Principale azienda

Area 'sistemi di elaborazione elettronica'.

E' responsabile per la strumentazione elettronica per le seguenti sedi:

- Sale prove C/o Scuola Don Minzoni
- Sede Principale azienda

L'ambito di applicazione della presente nomina non è legato a specifiche banche dati; l'operato del responsabile si dovrà mantenere nei limiti delle indicazioni prescritte nell'Allegato 1.

Il Responsabile dichiara di aver preso visione dei compiti assegnatigli (Allegato 1, codice documento 7566.4.75202.284934) e di essere a conoscenza delle disposizioni di legge contenute nel Codice della Privacy, con particolare riferimento agli obblighi inerenti al proprio mandato: si impegna pertanto ad adottare tutte le misure necessarie all'attuazione di tali norme.

L'incaricato del Trattamento dovrà osservare scrupolosamente tutte le istruzioni ricevute e le misure di sicurezza già in atto, o che verranno comunicate in seguito dal titolare (o dal responsabile se nominato) del trattamento.

Per accettazione

ELVIO AROSIO



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

Compiti del responsabile

La Legge definisce come responsabile "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali".

I confini generali di tale ruolo vengono delineati dal combinato disposto degli articoli 4 e 29 del codice, ai sensi dei quali si definisce responsabile il soggetto preposto dal titolare al trattamento dei dati personali, che deve essere individuato tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Tale soggetto deve quindi possedere una competenza insieme tecnica, legale in materia di privacy ed organizzativa.

Sicurezza

L'area 'sicurezza' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni inerenti alla implementazione delle misure di sicurezza atte a proteggere in modo preventivo e idoneo (art. 31 del Codice) i dati personali oggetto di trattamento e, in particolare, delle Misure Minime di Sicurezza trattate dagli artt. 33, 34, 35, 36 e dall'Allegato Disciplinare Tecnico B, ponendo estrema attenzione ai trattamenti di dati sensibili e giudiziari:

E' compito del Responsabile individuare e nominare, se lo ritiene opportuno, un Amministratore di Sistema ed eventualmente un incaricato alla custodia delle copie credenziali. E' altresì suo compito nominare eventualmente un incaricato al controllo degli accessi ai locali e obbligatoriamente un incaricato alla sorveglianza dell'archivio ad accesso autorizzato se dovessero esistere all'interno della struttura del Titolare archivi cartacei o contenitori di supporti informatici rimuovibili, contenenti dati sensibili o giudiziari.

Se il Responsabile della sicurezza decidesse di non nominare nessun amministratore di sistema od incaricato, se ne assumerà interamente le funzioni, i compiti e le responsabilità in relazione alla sicurezza dei dati personali.

È compito del Responsabile della Sicurezza:

- Se il trattamento dei dati personali è effettuato con l'ausilio di strumenti informatici, censire tutti i sistemi di elaborazione elettronica indicandone le caratteristiche principali (sistemi operativi, gestione multiprofilo, programmi di protezione, sistemi di antintrusione, programmi di elaborazione dei dati) e aggiornare, con cadenza annuale, l'elenco di tali sistemi.
- Individuare la dislocazione fisica dei trattamenti e in particolare:
 - le aree e i locali nei quali si trovano gli elaboratori o i sistemi di accesso remoto alle banche dati elettroniche e in particolare i sistemi che consentono l'accesso a dati sensibili o giudiziari; per tali aree e locali è bene nominare un incaricato al controllo accessi.
 - gli uffici e gli archivi nei quali vengono trattati e riposti dati sensibili o giudiziari; per tali archivi è necessario nominare un incaricato alla sorveglianza.
- Definire e verificare le modalità di accesso a tali locali e le misure da adottare per la protezione dei medesimi:
 - predisponendo i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati nonché le procedure per controllare l'accesso delle persone autorizzate;
 - impartendo specifiche istruzioni agli incaricati al controllo e alla sorveglianza delle aree e dei locali nonché degli archivi contenenti dati sensibili o giudiziari.
- Rendere esecutive tutte le misure di sicurezza adottate per la protezione dei dati personali e verificare la loro corretta implementazione con cadenza, almeno, semestrale.
- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate anche all'esterno nel caso venga affidato a terzi il trattamento dei propri dati personali; collaborare in tal senso con il Responsabile all'area 'trattamento dati' che ha compiti specifici.
- Predisporre ed aggiornare, entro il 31 Marzo di ogni anno, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi e produrre un piano di miglioramento incrementale di sicurezza (risk management) anche in base alle innovazioni tecnologiche in materia di protezione dei sistemi di elaborazione automatica e delle reti informatiche;
- Definire i criteri e le procedure per la sicurezza delle trasmissioni dei dati siano esse fatte attraverso fax o posta elettronica, ivi compresi quelli per le restrizioni di accesso per via telematica;
- Definire la politica di accesso alla rete da parte dei dipendenti, le loro responsabilità e le restrizioni in ordine alla sicurezza. Raccogliere, eventualmente, presso i dipendenti una assunzione di responsabilità per i siti visitati, nel caso venga loro concesso di navigare per proprio ed esclusivo interesse durante l'orario di lavoro.

- Relativamente alle disposizioni del punto precedente, è opportuno definire le modalità di gestione dei files di LOG da parte della direzione, fornendo a tal proposito espressa informativa e richiesta di consenso al trattamento dei medesimi: è da considerare il fatto che nei file di log siano contenuti dati personali anche sensibili. La direzione deve tenere in considerazione che il controllo dei log files rientra nelle disposizioni contenute nello Statuto dei Lavoratori art. 4 (Sorveglianza sul posto di lavoro).
- Custodire i supporti informatici adibiti alle copie di sicurezza dei dati impartendo istruzioni all'Amministratore di Sistema o all'incaricato della gestione e della manutenzione del sistema.
- Pianificare ed eseguire di test del sistema di sicurezza, attraverso adeguate prove di penetrazione
- Definire ed attuare di piani e strumenti di monitoraggio continuo della sicurezza
- Aggiornare periodicamente il sistema di sicurezza, per renderlo sempre adeguato alle nuove minacce
- Mantenere il sistema di sicurezza, per assicurarne costante efficienza e disponibilità
- Fornire supporto alla formazione del personale dell'organizzazione, in tema di sicurezza
- Emanare procedure interne inerenti la sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, ecc).
- Distruggere in modo definitivo i supporti rimovibili informatici destinati ad essere cestinati con particolare attenzione a quelli che contenevano dati personali sensibili;
- Distruggere le memorie fisse (Hard Disk) dei PC che eventualmente vanno in rottamazione.

Gestione dei sistemi di elaborazione elettronica.

L'area 'sistemi di elaborazione elettronica' comprende l'espletamento di tutte le operazioni inerenti alla gestione e alla manutenzione del sistema informatico non solo in rapporto alle soluzioni tecnologiche ma anche in ordine alle disposizioni di Legge in materia di sicurezza dei dati.

È compito del Responsabile individuare e nominare, se lo ritiene opportuno, uno o più incaricati alla manutenzione del sistema. Deve collaborare con gli altri responsabili nell'individuare e nominare gli incaricati al Back-up dei dati personali.

Se il Responsabile decidesse di non nominare nessun incaricato se ne assumerà le funzioni, i compiti e le responsabilità interamente.

È compito del Responsabile:

- Se il trattamento avviene con l'ausilio di mezzi informatici, deve redigere e aggiornare l'elenco dei sistemi hardware e software interessati al trattamento dei dati personali
- Attivare e gestire le credenziali di autenticazione degli incaricati ai trattamenti collaborando col Responsabile all'area 'trattamento dati' e col Responsabile alla sicurezza.
- Istruire gli incaricati dei trattamenti sull'uso delle parole chiave e sulle modalità per la modifica in autonomia, facendo riferimento al punto 3 delle istruzioni per l'incaricato dei trattamenti.
- Revocare e disattivare le credenziali di autenticazione agli incaricati che per qualunque motivo perdano la loro qualifica di incaricato
- Collaborare con il responsabile del trattamento nella definizione dei profili di autorizzazione definendo i trattamenti consentiti.
- Definire le politiche di protezione dei sistemi verso l'attacco di programmi (Virus) per tutte le basi dati elettroniche;
- Installare su tutte le postazioni client, sui server, sui PC e dove necessario (limitatamente all'ambito di competenza a lei assegnato) gli antivirus e aggiornarli con cadenza almeno semestrale! Si consiglia una frequenza del tutto più restrittiva.
- Effettuare tutti gli aggiornamenti patch dei sistemi operativi e dei programmi utilizzati per il trattamento dati, con cadenza annuale che diviene semestrale in caso di trattamenti di dati sensibili o giudiziari.
- Definire le politiche di protezione passiva della rete (firewall e sua configurazione) per la difesa del sistema dall'attacco di hackers.
- Verificare l'efficacia delle politiche di sicurezza almeno con cadenza semestrale.
- Collaborare con gli altri responsabili mantenendoli informati della gestione e di eventuali anomalie di sistema che potrebbero compromettere la sicurezza.
- Istruire gli incaricati dei back-up riguardo alle procedure da adottare per le operazioni di salvataggio delle copie di sicurezza dei dati personali, redigendo apposito documento di istruzioni. Risolvere gli eventuali problemi tecnici nella realizzazione dei back-up rilevati dai rispettivi incaricati.
- Sottoscrivere il documento con le istruzioni per il back up, conservarlo in luogo sicuro e trasmetterlo in copia agli incaricati del trattamento dei dati interessati alle copie di salvataggio, nonché all'incaricato dei back up di quella base dati. Per ogni base dati deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up e le modalità di custodia.
- Istruire l'incaricato alla manutenzione del sistema affinché le operazioni di riparazione e ripristino avvengano nel rispetto delle disposizioni di legge: in particolare dovrà attivare le necessarie azioni previste in caso gli elaboratori vengano spediti verso altra struttura per essere sottoposti alle necessarie riparazioni (vedi Trattamento terzi, clausole contrattuali) anche in collaborazione con il Responsabile dei trattamenti.

Rapporto con gli Interessati

L'area 'rapporto con gli interessati' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni volte a

soddisfare i diritti sanciti dall'art.7 del Codice della privacy.

È compito del Responsabile:

- Conoscere i modi e i tempi entro i quali venire incontro alle richieste dell'interessato (artt.7, 8, 146).
- Prendere in carico tempestivamente e non oltre le 24 ore successive al loro ricevimento, i reclami degli interessati e le eventuali istanze del garante.
- Effettuare la ricerca dei dati richiesti, producendone una copia rispondente ai criteri di intelleggibilità e chiarezza stabiliti dalla legge.
- Informare il titolare nel caso in cui dovessero intervenire delle difficoltà nella raccolta dei dati tali da compromettere in parte o del tutto la buona riuscita dell'operazione.



GAIN STUDIOS DI AROSIO ELVIO S.A.S.

Viale Montegrappa 28/G - 27100 - PAVIA (PV)

Tel: 0382 464161 - Fax: 0382 464161

p.Iva 01941490185

Il Titolare

Titolare : GAIN STUDIOS DI AROSIO ELVIO S.A.S. nella persona di ELVIO AROSIO

La Legge definisce come titolare la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Al titolare spettano, per presunzione assoluta di legge, la direzione delle attività di trattamento dei dati personali: a tale soggetto competono infatti le decisioni strategiche di fondo su come (modalità) e perché (finalità) raccogliere e trattare i dati, nonché sull'organizzazione del trattamento e sulle risorse (strumenti) da dedicarvi, anche per garantire la sicurezza. Il titolare si identifica con la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo cui oggettivamente spettano tali decisioni di fondo.

Nel caso di persone giuridiche, tale figura tende in generale a coincidere con il legale rappresentante della società o dell'ente potendosi così individuare, anche nell'ambito di strutture complesse, chi sia specificamente: tale soggetto sarà sempre e comunque tenuto in prima persona a rispondere per i danni cagionati nel trattamento dei dati, nonché delle sanzioni di carattere civilistico ed amministrativo.

E' inoltre possibile che, da parte delle autorità preposte all'accertamento degli eventuali reati, le responsabilità di ordine penale vengano estese a tutti i componenti dell'organo cui spetta la direzione della società e dell'ente (ad esempio, i membri del Consiglio di Amministrazione).

Compiti del Titolare

E' compito del titolare:

- Mettere in atto e verificare l'applicazione di tutte le disposizioni di legge in ordine ai trattamenti di dati personali in corso.
- Adottare e verificare l'implementazione delle misure di sicurezza previste dal Codice della Privacy per garantire l'idonea protezione ai dati, ponendo particolare attenzione alle misure minime di sicurezza.
- Individuare e nominare gli incaricati ai trattamenti di dati personali, per iscritto e fornendo loro istruzioni per poter operare in modo corretto e secondo quanto disposto dal Codice della Privacy anche in riferimento alle misure di sicurezza.
- Eventualmente individuare e nominare dei responsabili tramite lettera di nomina scritta definendo le aree di competenza (trattamento dei dati, sicurezza, gestione dei sistemi di elaborazione elettronica, rapporto con gli interessati) e i compiti assegnati.
- Provvedere a fornire a Responsabili e Incaricati l'adeguata istruzione riguardo le disposizioni di legge contenute nel Codice della Privacy che regolano le responsabilità, le funzioni e gli scopi propri della loro mansione nonché le norme basilari relative ai trattamenti e alla protezione dei dati.
- Il Titolare del trattamento può ritenere di non nominare alcun responsabile con la consapevolezza di accollarsi per intero le responsabilità e le funzioni loro proprie. In questo caso sarà sua preoccupazione realizzare l'intero adeguamento di Legge secondo tutte le norme e le disposizioni in essa contenute.

In particolare, non essendo stati nominati dei Responsabili in tutte le aree di competenza, sono sotto riportati , divisi per aree di competenza, i compiti che devono essere eseguiti dal titolare, almeno fino alla nomina dei relativi Responsabili.

Trattamento dei dati

L'area 'trattamento dati' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni inerenti alla gestione dei rapporti tra il Titolare e il Garante, tra il Titolare e gli interessati, e alla gestione operativa dei trattamenti dei dati personali:

- gestione notifica
- gestione rapporti con il Garante
- verifica corrispondenza con Autorizzazioni Annuali

- gestione comunicazione e diffusione dei dati secondo legge
- gestione informativa e consenso verso interessati
- gestione diritti di accesso degli interessati
- gestione delle modalità dei trattamenti interni
- nomina degli incaricati del trattamento
- creazione e gestione dei profili di autorizzazione
- gestione dei trattamenti affidati a terzi
- gestione della formazione da impartire agli incaricati

Individuare e nominare Incaricati dei trattamenti tutti coloro che sono addetti al trattamento esecutivo dei dati personali.

È compito del Responsabile ai Trattamenti:

- Raggiungere un sufficiente grado di apprendimento in materia di Privacy in modo da poter trattare i dati secondo la Legge e realmente vigilare sulla liceità e sulla correttezza dei trattamenti.
- Predisporre la notificazione iniziale al Garante nel caso in cui il trattamento rientri nei casi contemplati dall'art.37 del Codice, attraverso il programma Web disponibile sul sito del Garante (www.garanteprivacy.it), verificando l'esattezza e la completezza dei dati contenuti.
- Interagire con il Garante, in caso di richieste di informazioni o effettuazione di controlli ed accessi da parte dell'autorità;
- Censire analiticamente le banche dati con tutti gli elementi necessari per la determinazione dei trattamenti e delle tipologie di dati da inserire nel DPSS (dati trattati, tipi di trattamento, categorie di interessati, sedi e uffici del trattamento e in collaborazione con il Responsabile della Sicurezza, l'elenco dei sistemi di elaborazione nei quali avvengono i trattamenti), anche ai fini della eventuale notifica al Garante;
- Verificare che i trattamenti dei dati sensibili rientrino nelle Autorizzazioni del Garante in corso di validità ed, eventualmente, predisporre la richiesta di autorizzazione preventiva al trattamento di dati sensibili nel caso in cui il trattamento non rientri in tali Autorizzazioni.
- Procedere alla gestione delle informative e delle richieste di consenso nei casi e nelle modalità previste dalla legge
- Gestire il diritto di accesso degli interessati, agendo prontamente per soddisfare le loro richieste secondo l'art. 7; a questo proposito il Responsabile del trattamento ha la facoltà di nominare un Responsabile del Diritto di Accesso, al quale può delegare tale compito.
- Aggiornare l'elenco dei trattamenti in relazione ad eventuali nuovi trattamenti di dati personali;
- Individuare e nominare gli incaricati del trattamento impartendo loro, per iscritto, la nomina, le istruzioni e le autorizzazioni necessarie ad un corretto, lecito e sicuro trattamento, verificandone la puntuale applicazione;
- Produrre le nomine, le istruzioni e la distribuzione dei compiti (mansionario privacy) da consegnare ai medesimi per la firma e l'archiviazione.
- Collaborare con eventuali altri Responsabili e con l'eventuale Amministratore di Sistema.
- Definire i profili di autorizzazione (ambiti di competenza e operazioni consentite) degli incaricati
- Autorizzare i singoli incaricati al trattamento specifico di dati sensibili e giudiziari ponendo bene in evidenza tale fatto nella definizione del profilo di autorizzazione;
- Tenere aggiornato l'elenco dei trattamenti (censimento delle banche dati, tipologie di dati trattati, sedi in cui vengono trattati) e la distribuzione dei compiti (mansionario della privacy), con cadenza almeno annuale.
- Periodicamente con cadenza almeno annuale verificare la correttezza dei profili di autorizzazione revisionando gli ambiti di competenza ed eventualmente adattandoli a nuove esigenze.
- Provvedere a eliminare le autorizzazioni che rimangono inutilizzate oltre i sei mesi, sempre che il profilo particolare non determini per propria definizione un trattamento sporadico.
- Attuare gli obblighi di informazione ad acquisizione del consenso, quando richiesto, nei confronti degli interessati; delegare eventualmente questa incombenza ai singoli incaricati. A tal fine è possibile utilizzare i moduli e le procedure predisposte attraverso il Portale della Privacy.
- Individuare i trattamenti che vengono ceduti a Terzi (ad es. la gestione delle paghe) e attuare i necessari provvedimenti affinché tali trattamenti avvengano secondo liceità e correttezza garantendo lo standard di sicurezza previsto dalla legge. Il Responsabile deve decidere se nominare Responsabile la società terza in oggetto, se nominare Incaricati i soggetti individuali terzi che materialmente effettueranno i trattamenti o se introdurre restrittive clausole di garanzia nel contratto di fornitura del servizio. In queste operazioni può collaborare con l'eventuale Responsabile dell'area sicurezza.
- Verificare che tutti i trattamenti avvengano nel rispetto delle disposizioni di legge.
- Distruggere i dati personali che non sono più oggetto di trattamento alcuno.
- Informare prontamente il Titolare ed il personale interno addetto alla privacy di ogni questione rilevante ai fini di legge;
- Comunicare al Titolare qualsiasi elemento oggettivo o soggettivo che possa compromettere il corretto trattamento dei dati personali.
- Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del Titolare; nel caso venga delegato il trattamento all'esterno gestire il trattamento tramite terzi attuando le misure necessarie affinché sia garantita la sicurezza dei dati esportati, questo anche in collaborazione con l'eventuale Responsabile dell'area sicurezza.
- Collaborare con l'eventuale Responsabile dell'area sicurezza e con l'eventuale Amministratore di Sistema nella definizione delle credenziali di autenticazione e dei profili di autorizzazione.
- Elaborare un piano di formazione per rendere edotti gli incaricati del trattamento delle disposizioni di legge sulle modalità e i criteri del trattamento, nonché dei rischi individuati e dei modi per prevenire danni, anche in collaborazione con gli altri Responsabili.
- Collaborare con tutti i responsabili per l'attuazione delle prescrizioni impartite dal Garante attraverso nuove circolari,

- autorizzazioni e aggiornamenti di Legge;
- Gestire la cifratura e la separazione nei casi in cui vi sia la coesistenza di dati identificativi dell'interessato e dati sensibili, con particolare riferimento a quelli sanitari, che consentano una immediata associazione tra di essi. E' possibile fare riferimento alle soluzioni proposte dal Portale della Privacy.