Zona Industriale III Fase, Viale 15 n°2 97100 Ragusa | Tel. 0932 667666 - Fax 0932667929
info@novaquadri.it | grupponovaquadri@pec.it | novaquadri.it

Modello Organizzativo Privacy

Ver 2.4

18/02/2026

Il presente documento è stato redatto in base alle ultime disposizioni legislative finalizzata all'allineamento dei principi sanciti nel Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Scopo del presente documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati personali effettuato dai soggetti contitolari (di seguito “Gruppo”). secondo quanto previsto dall’art 26 del Regolamento UE 2016/679.

Definizioni Principali Normativa Privacy

Titolare del Trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del Trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Addetti del Trattamento: le persone fisiche autorizzate a compiere operazioni di trattamento da titolare o dal responsabile.

Interessato: la persona fisica a cui si riferiscono i dati personali (tutti noi siamo interessati).

Destinatario: la persona fisica o giuridica, l'autorità pubblica; il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dato sensibile: 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 rilevare lo stato di salute e la vita sessuale.

Dato giudiziario: i dati personali idonei a rivelare informazioni 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 biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Principi Generali Adottati dall'Organizzazione

Ogni Titolare è tenuto a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Obblighi di sicurezza

Ogni Titolare è tenuto a garantire che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base allo stato dell'arte e all'avanzamento tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Misure di Sicurezza Idonee

Ogni Titolare è tenuto ad adottare un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza per assicurare un livello idoneo di protezione dei dati personali sia nel caso di trattamenti con strumenti elettronici che per trattamenti senza l'ausilio di strumenti elettronici.

Dati Generali (Tabella 1)

Titolare del trattamento	**GRUPPO NOVA QUADRI – Rete di imprese** P. IVA 01797550884**,** nella persona del legale rappresentante sig. Roberto Russo, con sede in Ragusa, Zona Ind.le III Fase, Viale 15, n. 2;

Responsabili del trattamento	1. **NQ ITALIA S.R.L.** P. IVA 01473720884**,** in persona del legale rappresentante sig. Ciro Lambro, con sede in Ragusa, Zona Ind.le III Fase, Viale 15, n. 2 2. **BLUNOVA SRL** P.IVA 01050370889**,** in persona del legale rappresentante sig.ra Vincenza Occhipinti, con sede in Ragusa, Zona Ind.le III Fase, Viale 15, n. 2 3. **PROTELI S.R.L.** P.IVA 01424640884**,** in persona del legale rappresentante sig. Roberto Russo, con sede in Ragusa, Zona Ind.le III Fase, Viale 15, n. 2 4. **S.T.I. PROGET S.R.L. SOCIETA' DI INGEGNERIA** P. IVA 01008110882**,** in persona del legale rappresentante Giuseppe Firullo, con sede in Ragusa, Zona Ind.le III Fase, Viale 15, n. 2 5. **INNOVA S.R.L.** P. IVA 01707520886**,** in persona del legale rappresentante Ciro Lambro, con sede in Ragusa, Zona Ind.le III Fase, Viale 15, n. 2 6. **GRILLER CHEF S.R.L.S.** P. IVA 01694950880, in persona del legale rappresentante Antonio D'Asta, con sede in Via Vanella 47 n°20/c, 971015 Modica **7. BLUNOVA TRAPANI S.R.L.S.** P. IVA 02693260818, in persona del legale rappresentante Salvatore Todaro, con sede in Via Mazara, 13, 91100 Trapani

	8. **Ditta RAPICANO PATRIZIA** P.IVA IT01276310883 nella persona del legale rappresentante Patrizia Rapicano, via Ugo La Malfa n. 47 RAGUSA 9. **ICONTROL S.R.L.S.** P.IVA 01683580888 in persona del legale rappresentante Mauro Civello, C.DA Fossa Samuele 2, 97018 Scicli (RG)

Zona Industriale III Fase, Viale 15 n°2 97100 Ragusa | Tel. 0932 667666 - Fax 0932667929
info@novaquadri.it | grupponovaquadri@pec.it | novaquadri.it

Censimento e gestione delle banche dati

BANCA DATI		**Gestione Clienti**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	NO
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Gestione fornitori**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	NO
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Contabilità, cedolini, buste paga e certificazioni fiscali**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	NO
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Gestione Dipendenti e Collaboratori**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	SI
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Adempimenti di sicurezza, sanità e prevenzione**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	SI
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	SI

BANCA DATI		**Adempimenti previsti dal Reg. EU 679/16 (privacy)**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	SI
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	SI

BANCA DATI		**Gestionale SIQSA**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	NO
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Gestione connettività clienti (Rubrica RADIUS)**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	NO
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Gestione gare e appalti**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	NO
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Adempimenti ed azioni legali**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	NO
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Geolocalizzazione Veicoli**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	SI	CONSERVAZIONE	SI
ADATTAMENTO	SI	MODIFICA	SI
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	NO
DIFFUSIONE	NO	RAFFRONTO	SI
INTERCONNESSIONE	SI	LIMITAZIONE	SI
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

BANCA DATI		**Videosorveglianza**	
RACCOLTA	SI	REGISTRAZIONE	SI
STRUTTURAZIONE	NO	CONSERVAZIONE	NO
ADATTAMENTO	NO	MODIFICA	NO
CONSULTAZIONE	SI	ESTRAZIONE	SI
USO	SI	COMUNICAZIONE	SI
DIFFUSIONE	NO	RAFFRONTO	NO
INTERCONNESSIONE	NO	LIMITAZIONE	NO
CANCELLAZIONE	SI	DISTRIBUZIONE	NO

Trattamenti affidati all'esterno

Ogni Titolare del trattamento relativamente ad alcuni trattamenti di dati, ha affidato la loro gestione a soggetti esterni designandoli formalmente con apposita lettera di nomina.

Di seguito sono sintetizzati i criteri e gli impegni assunti dalle parti esterne all'organizzazione, per l'adozione delle misure di sicurezza, affinché venga garantito un adeguato trattamento.

Banca dati affidata in outsourcing	Adempimenti e azioni legali
Soggetto esterno	Avv. Samantha Nicosia

Descrizione dei criteri e degli impegni assunti per l'adozione delle misure minime di sicurezza (Tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale)
Adempimenti degli obblighi previsti dal Codice per la protezione dei dati personali Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – ed informare immediatamente Ogni Titolare del trattamento in caso di situazioni anomale o di emergenze. Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto

Banca dati affidata in outsourcing	Contabilità Cedolini buste paga e certificazioni fiscali
Soggetto esterno	Dott. Claudio CAPPELLO
Descrizione dei criteri e degli impegni assunti per l'adozione delle misure minime di sicurezza (Tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale)	
Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto Adempimenti degli obblighi previsti dal Codice per la protezione dei dati personali Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – ed informare immediatamente il Titolare indicato nell'incarico in caso di situazioni anomale o di emergenze.	

Banca dati affidata in outsourcing	Adempimenti sanitari
Soggetto esterno	Dr. Mario D'Asta
Descrizione dei criteri e degli impegni assunti per l'adozione delle misure minime di sicurezza (Tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale)	
Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto Adempimenti degli obblighi previsti dal Codice per la protezione dei dati personali Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – ed informare immediatamente il Titolare indicato nell'incarico in caso di situazioni anomale o di emergenze.	

Banca dati affidata in outsourcing	Cedolini buste paga e certificazioni fiscali Adempimenti sicurezza e prevenzione Anagrafica Dipendenti e Collaboratori
Soggetto esterno	Dott.ssa Rosaria Gurrieri Amalia La Terra

Zona Industriale III Fase, Viale 15 n°2 97100 Ragusa | Tel. 0932 667666 - Fax 0932667929
info@novaquadri.it | grupponovaquadri@pec.it | novaquadri.it

Descrizione dei criteri e degli impegni assunti per l'adozione delle misure minime di sicurezza (Tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale)
Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto
Adempimenti degli obblighi previsti dal Codice per la protezione dei dati personali
Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento
Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – ed informare immediatamente il Titolare indicato nell'incarico in caso di situazioni anomale o di emergenze.

Procedura per l'accesso, la conservazione e la cancellazione

Accesso ai dati

Ogni Titolare ha identificato come categorie di interessati le seguenti categorie:

- CLIENTI
- FORNITORI
- DIPENDENTI E COLLABORATORI
- TERZE PARTI

Tutti i dati trattati da tali categorie sono accessibili al solo personale debitamente formato e nominato con apposita lettera di nomina e vengono gestiti elettronicamente tramite il gestionale per la contabilità. A livello cartaceo sono riposti in archivi specifici divisi per area; quindi ha istruito il personale di riferimento sulla comunicazione immediata dei dati qualora ne venga fatta la richiesta da un interessato.

In tal senso viene consentito agli interessati di accedere ai propri dati per:

- Verificarne la veridicità;
- Modificarli nel caso divengano inesatti;
- Integrarli anche con dichiarazione integrativa;
- Richiederne la cancellazione, ove non sussistano specifici obblighi di legge che ne richiedano la conservazione;

Accesso ai dati personali: l'accesso ai dati personali è libero per gli autorizzati al trattamento dei dati, persone non autorizzate che dovranno accedere alla zona dell'archivio dovranno essere accompagnate per evitare l'accesso non consentito ai dati.

Accesso a particolari categorie di dati (ex art 9 GDPR): l'accesso agli archivi contenenti dati sensibili è consentito esclusivamente a persone autorizzate. Non sono ammesse persone, anche se autorizzate, dopo l'orario di chiusura.

Conservazione dei dati

Ogni Responsabile conserverà i dati degli interessati in una forma che consenta l'identificazione degli stessi per un arco temporale non superiore al conseguimento delle finalità per le quali sono stati raccolti.

I dati strettamente necessari per gli adempimenti fiscali, contabili e per la gestione del rapporto di lavoro, venuta meno la finalità per la quale erano stati raccolti, verranno comunque conservati secondo disposizioni di cui all'art. 22 del DPR n. 600/1973, comunque per un periodo non superiore a 10 anni salvo diverse disposizioni di legge.

UFFICIO / AREA	TIPO TRATTAMENTO	PERIODO CONSERVAZIONE	BASE GIURIDICA
Area Legale	Tutela in sede giudiziaria	10 anni	Legittimo interesse del titolare
Area Legale	Adempimenti di legge	Vincolato a base giuridica	Obbligo di legge e/o regolamento
Ufficio Amministrazione	Gestione buste paga e certificazioni fiscali	Vincolato a base giuridica	Obbligo di legge e/o regolamento

Ufficio Amministrazione	Selezione del personale (curriculum vitae)	2 anni	Legittimo interesse del titolare
Ufficio Amministrazione	Assunzione del personale	10 anni	Esecuzione di un contratto ovvero Consenso dell'interessato
Ufficio Amministrazione	Gestione dipendenti e collaboratori	Vincolato a normativa giuslavoristica e previdenziale	Esecuzione di contratto tra le parti ovvero Obbligo di legge
Area Commerciale	Marketing vs. potenziali clienti	2 anni	Consenso dell'interessato
Area Commerciale	Marketing vs. clienti attivi	Vincolato a durata del contratto	Legittimo interesse del titolare
Ufficio Amministrazione	Cessazione dipendenti e/o collaboratori	10 anni	Legittimo interesse del titolare
Area Tecnica	Esecuzione installazioni	10 anni	Esecuzione di contratto tra le parti
Ufficio Gare	Gestione appalti e/o gare	10 anni	Consenso dell'interessato
Sicurezza e prevenzione	Gestione adempimenti sicurezza	Vincolato a base giuridica	Obbligo di legge e/o regolamento

Cancellazione dei dati

Ogni Titolare, in osservanza al corrispondente diritto di accesso all'interessato, ha predisposto procedure per le quali gli interessati possano richiedere la cancellazione senza ingiustificato ritardo dei dati personali o limitazione del trattamento dei dati personali che li riguardano per i seguenti motivi:

- Perché i dati non sono più necessari per la finalità per i quali erano stati raccolti;
- Perché il periodo di conservazione è giunto al termine;
- Perché la base giuridica per la quale erano stati raccolti non è più valida;
- Perché l'interessato ha revocato il consenso al trattamento dei dati;
- Perché l'interessato si oppone al trattamento;
- Perché i dati sono trattati illecitamente;

Ogni Titolare ha previsto quindi che nei casi sopra citati il termine ultimo per la cancellazione sia di massimo 30 giorni dalla data di accertamento dell'irregolarità.

Sono state predisposte verifiche periodiche da parte dei relativi responsabili del trattamento, con cadenza semestrale.

Analisi dei rischi del trattamento

Analisi dei rischi				
Contesto	**Rischio**	**Probabilità**	**Gravità dell'evento incidente**	**Misure di contenimento del rischio**
Personale dipendente e collaboratori	Uso improprio delle credenziali aziendali	Media	Media	Blocco account
	Scarsa accuratezza dei dati acquisiti	Media	Bassa	Valutazione e Formazione periodica del personale
	Comportamenti sleali o fraudolenti	Bassa	Alta	Gestione centralizzata dei log applicativi e sistemistici Videosorveglianza di sede
	Errore Umano	Media	Alta	Formazione Backup periodici Copie cartacee d'archivio
Tecnologie e processi	Azione di virus informatici	Alta	Alta	Antivirus aggiornato Segregazione dei privilegi operativi degli utenti
	Spamming / Denial of Service	Media	Alta	Virtualizzazione e ridondanza dei sistemi informativi e

				dell'accesso a internet
	Malfunzionamento, indisponibilità o degrado degli strumenti	Bassa	Media	Ridondanza dei sistemi e delle applicazioni
	Accessi esterni non autorizzati	Bassa	Alta	Firewall aziendale
	Intercettazione di informazioni in rete	Alta	Bassa	Antivirus / antimalware aggiornato Proxy
Sicurezza fisica	Accessi non autorizzati a locali/reparti ad accesso ristretto	Bassa	Media	Autenticazione postazioni di lavoro Videosorveglianza
	Asportazione e furto di strumenti contenenti dati	Bassa	Alta	Videosorveglianza
	Guasto ai sistemi complementari (impianto elettrico, idrico, ecc.)	Bassa	Media	Manutenzione periodica Ridondanza sistemi
	Errori umani nella gestione della sicurezza dati	Media	Media	Verifica e formazione periodica del personale

Misure di sicurezza idonee adottate al livello cartaceo

Procedure di Custodia Atti e Documenti

- **Dati Comuni**: l'archivio degli atti e dei documenti contenente dati personali è consentito al solo personale autorizzato e debitamente formato in un'area alla quale non è permesso l'accesso libero a persone non autorizzate al trattamento dei dati.
- **Accesso a dati di categorie particolari ex art 9**: L'accesso agli archivi contenenti dati sensibili è consentito esclusivamente a persone autorizzate e dotate di chiave d'accesso alla cassaforte, la cui assegnazione è specificata nella lettera d'incarico al trattamento dati. Non sono ammesse persone, anche se autorizzate, dopo l'orario di chiusura.

Gli atti e i documenti sono conservati presso la nostra sede di cui sotto elenchiamo le caratteristiche:

Sede Gruppo Nova Quadri, Piano Terra.

Sede Gruppo Nova Quadri, Piano seminterrato

Gli atti e i documenti quando sono prelevati per essere utilizzati dovranno essere rimessi al loro posto prima dell'orario di chiusura.

Misure di Sicurezza idonee adottate a livello elettronico

L'operatore potrà accedere ai computer ai quali è autorizzato esclusivamente inserendo le proprie credenziali e la propria password. L'addetto non potrà diminuire il livello di sicurezza stabilito dall'amministratore di sistema per il computer a cui accede.

L'addetto dovrà operare con diligenza ponendo estrema cura ed attenzione nell'utilizzo del computer e delle applicazioni al fine di evitare cancellazioni e modifiche errate, accidentali o intenzionali che possono arrecare danno o pregiudizio alla nostra organizzazione e per le quali sarà ritenuto responsabile.

L'addetto dovrà segnalate immediatamente al responsabile del trattamento dati eventuali anomalie di funzionamento dei computer, della rete del computer e delle applicazioni utilizzate.

L'elenco dei dispositivi elettronici censiti dai Titolari è presente in apposito documento excel, denominato **"AssetList_GruppoNovaQuadri"** ed è aggiornato semestralmente dagli amministratori di sistema.

Sistema di Autenticazione

Utilizzo di username e password integrati a dominio. L'utente ricorda la propria username e la propria password che sono anche memorizzate sul sistema di accesso. Per un buon utilizzo della password è stato distribuito a tutti gli incaricati il Disciplinare per l'utilizzo di posta elettronica, internet e postazioni di lavoro.

Sistema di Autorizzazione

Autorizzazioni all'accesso ai dati secondo diversi livelli di responsabilità, limitate alle sole parti di trattamento per le quali sono stati assegnati compiti agli addetti con limitazioni specifiche per ogni Singolo addetto.

Protezione da accessi non consentiti

Nel caso di accessi non autorizzati verranno immediatamente bloccate tutte le operazioni su tutti i Computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tutte le connessioni con internet e verrà controllata tutta la rete dei computer, tutti i sistemi operativi, tutti software installati e tutti i dati inseriti per verificare eventuali danni provocati dagli accessi noti autorizzati e per il ripristinò della normalità.

Nel caso l'accesso non autorizzato sia stato effettuato per scopi fraudolenti o di sabotaggio si provvederà all'immediata denuncia presso le forze di polizia e/o l'autorità giudiziaria dell'eventuale responsabile degli accessi non autorizzati.

Nel caso l'accesso non autorizzato sia stato effettuato con scopi non conformi alle norme interne della nostra organizzazione ma comunque non a scopo fraudolento o di sabotaggio verranno adottati tutti i provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori delle norme sindacali, dalle norme deontologiche.

Per prevenire l'accesso ai dati da parte di operatori non autenticati l'addetto attiva tramite CTRL+ALT+CANC il blocco del computer, consentendo lo sblocco solo ad operatori autorizzati.

Protezione da trattamenti illeciti dei dati

I dati sono protetti da un sistema di autenticazione che concede l'accesso agli addetti autenticati attraverso il riconoscimento di password d'accesso ai dati e che concede l'accesso agli addetti ai soli ambiti di trattamento dati a loro consentiti.

Nel caso di carenza di consapevolezza, disattenzione o incuria degli addetti sarà bloccato temporaneamente l'accesso ai dati degli addetti e formato l'addetto sulle procedure del trattamento.

Nel caso di comportamenti sleali e fraudolenti degli addetti sarà bloccato immediatamente l'accesso ai dati degli addetti adottati i relativi provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.

Protezione da programmi informatici

Sulle postazioni di lavoro è attivo un software antivirus con aggiornamento automatico.

Non è attiva la gestione centralizzata dell'antivirus sulle Postazioni di Lavoro.

Nel caso di azione di virus informatici verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete attraverso l'utilizzo di un programma antivirus aggiornato e verrà immediatamente verificata e bonificata manualmente tutta la rete dei computer da parte dell'amministratore di sistema. Nel caso di azione dei programmi suscettibili di recare danno verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà i programmi dannosi e verrà immediatamente verificata e bonificata tutta la rete dei computer.

Procedure di backup

Le copie di backup vengono effettuate:

- Automaticamente con frequenza programmata

Procedure per la custodia delle copie di sicurezza

Le copia di backup dei dati sono conservate presso:

- CED, Piano Seminterrato

Le copie settimanali dei backup vengono portate fuori dalla sede dall'Amministratore di Sistema e da lui custodite. Le copie di backup sono accessibili esclusivamente ad operatori autorizzati.

Le più importanti misure di sicurezza da adottare, in caso di utilizzo di strumenti informatizzati

- Utilizzate sempre il codice identificativo personale e le parole chiave, cambiandole ogni qual volta abbiate la sensazione che esse non siano sufficientemente sicure; laddove possibile, utilizzate sempre almeno 8 caratteri, mescolando caratteri maiuscoli e minuscoli.

- La parola chiave deve essere preferibilmente priva di significato e non deve mai essere comunicata a soggetti terzi, anche se fiduciari.

- Ricordate che in caso di trattamento di dati sensibili la parola chiave deve essere cambiata almeno ogni tre mesi, e se questo intervallo viene ridotto, tanto meglio.

- Si raccomanda di evitare di utilizzare la stessa parola chiave sia sui computer portatili che su quelli fissi.

- Accertatevi di effettuare con frequenza la copia di backup dei dati archiviati sul personal computer o supporto di memoria asportabile, trasferendoli su supporti portatili (es. memoria usb). In questo caso, si faccia attenzione a che le modalità di custodia di questi supporti portatili siano quelle applicate al computer principale.

- Non tenete mai insieme le copie di backup ed il personal computer, per evitare che un eventuale furto possa coinvolgere sia i dati del personal computer che quelli di backup.

- Tutte le precauzioni che vengono prese all'interno del Gruppo per filtrare virus e messaggi di posta elettronica non autorizzati potrebbero non essere attive, quando il personal computer viene collegato a una presa telefonica di un albergo. Si faccia quindi particolare attenzione, quando ci si collega ad Internet attraverso reti non dotate di appropriati filtri, al tipo di messaggio che viene ricevuto.

- Ci si accerti che il software antivirus, presente sul personal computer, sia aggiornato con cadenza almeno quotidiana e ci si accerti che il sistema operativo ed altri applicativi residenti siano sempre aggiornati;

- Se scoprite che il vostro personal computer è infetto da virus, chiedete subito istruzioni al responsabile del trattamento sugli interventi da attuare, e non effettuate ulteriori elaborazioni.

- Collegatevi regolarmente al sito Internet del venditore degli applicativi residenti su personal computer, in modo da avere sempre a disposizione gli ultimi aggiornamenti, che molto spesso sono mirati non solo a migliorare la flessibilità d'uso dell'applicativo, ma anche e soprattutto la sua sicurezza.

- Non lasciate mai il personal computer collegato ad Internet senza il vostro presidio; anzi, cercate di tenervi collegati soltanto per il minimo tempo necessario per effettuare le operazioni desiderate.

- Non permettete ad alcuna persona, anche di fiducia di accedere al vostro personal computer.

Istruzioni agli addetti al trattamento che trattano dati con strumenti elettronici corredate di Linee Guida per la Prevenzione dei Virus e per la scelta delle password

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

1. **Riservatezza**: Prevenzione contro l'accesso non autorizzato alle informazioni
2. **Integrità:** Le informazioni non devono essere alterabili da incidenti o abusi
3. **Disponibilità**: Il sistema deve essere protetto da interruzioni impreviste

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi, misure soltanto tecniche, per quanto possono essere sofisticate, non saranno efficienti se non usate propriamente. In particolare, le precauzioni di tipo tecnologico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

- **Utilizzare le chiavi**: il primo livello dì protezione di qualunque sistema è quello fisico: è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario, non banale, per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio e riponete i documenti negli appositi contenitori alla fine di ogni giornata di lavoro.

- **Conservare i documenti in luoghi sicuri**: tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un identificativo ma mai con i nominativi di studenti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche. Tutti i contenitori con i documenti devono essere posti in scaffalature a giorno; se poste in luoghi controllati, o in armadi con serratura o ripostigli con porte con serratura se posti in luoghi non controllati o aperti al pubblico. I dati per cui viene richiesto il blocco o la cancellazione, che devono essere mantenuti per un obbligo di legge o a propria tutela in quanto relativi ad adempimenti contrattuali svolti, dovranno essere posti in armadi con serratura o ripostigli con porte con serratura. I dati sensibili o giudiziari dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serratura e sono consegnati agli incaricati sotto la loro responsabilità e, al di fuori dell'orario di lavoro, solo previa registrazione. I dati estremamente riservati dovranno essere posti in armadi blindati, casseforti o luoghi sicuri (locali in muratura con porta blindata). Non lasciare documenti con dati personali sui tavoli, dopo averli utilizzati; riponeteli sempre nei loro contenitori.

- **Conservare i CD in un luogo sicuro**: per i CD, DVD, dischetti, pen-drive e per qualsiasi altro supporto removibile di dati, si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può essere anche dovuto ad, un furto) può passare più facilmente inosservato. Riponeteli quindi sotto chiave in armadi o archivi non appena avete finito di usarli.

- **Utilizzate le password**: vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:
  - la password di accesso al computer che impedisce l'utilizzo improprio della vostra postazione quando per un motivo qualsiasi non vi trovate in ufficio;
  - la password di accesso alla rete che impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'ufficio;
  - la password di programmi specifici che impedisce l'accesso ai documenti realizzati con quelle applicazioni;
  - la password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta persona non autorizzata di visualizzare il vostro lavoro.

L'utilizzo di questi tipi fondamentali di password è obbligatorio. Imparatene l'utilizzo, e nel caso dobbiate comunicare, almeno temporaneamente, ai tecnici incaricati dell'assistenza, la vostra password registrate l'ora di comunicazione e di rinnovo della vostra password.

- **Attenzione alle stampe e ai fax di documenti riservati:** non lasciate accedere alle stampe o ai fax persone non autorizzate, se la stampante o il fax non si trovano sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Posizionate le stampanti e i fax in luoghi controllati e non accessibili al pubblico ed a visitatori. Distruggete personalmente le stampe quando non servono più. È opportuno l'utilizzo di una macchina distruggi documenti, indispensabile nel caso di documenti sensibili o giudiziari.

- **Non utilizzate le mail per dati riservati**: non inviate MAI dati riservati via email come numeri di carta di credito, password, numeri di conti bancari.

- **Prestate attenzione all'utilizzo dei computer portatili**: i computer portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido e utilizzate una procedura di backup periodico. Se durante la giornata vi spostate molto dalla vostra postazione o addirittura la notte lasciate il vostro portatile in ufficio, riponetelo in armadi chiusi a chiave.

- **Non fatevi spiare quando state digitando la password**: anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete una buona capacità di digitazione.

- **Custodite la password in un luogo sicuro**: scrivete la vostra password, chiudetela in busta chiusa e consegnatela all'incaricato addetto alla sua custodia che provvederà a firmarla nei lembi di chiusura. Fate ben attenzione a non riscrivere la vostra password, l'unico affidabile dispositivo di registrazione è la vostra memoria.

- **Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identità e delle loro autorizzazioni**: personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro computer.

- **Non utilizzate connessioni ad internet "hotspot"**: l'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer ma a tutti i dati dell'organizzazione. Per l'utilizzo consultatevi con il responsabile del trattamento dati.

- **Non installate programmi non autorizzati:** solo i programmi acquistati dalla vostra organizzazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici consultatevi con il responsabile del trattamento dati.

- **Adottate con cura le linee guida per la prevenzione di virus:** la prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di tutti i dati.

- **Controllate la politica locale relativa ai backup:** i vostri dati potrebbero essere gestiti su un server, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Chiedete al responsabile del trattamento dati quali sono le operazioni di backup che dovete eseguire, con quali modalità e con quali tempi. Il responsabile del trattamento curerà con estrema cura ed attenzione i backup periodici di tutti i dati.

- **Utilizzate gruppi di continuità:** verificare lo stato di funzionamento e l'effettiva attivazione di gruppi di continuità, se presenti.

- **Segnalate le anomalie:** segnalate sempre, al più presto, al responsabile del trattamento dati, qualsiasi tipo di anomalia si verifichi, sia nelle funzionalità del computer in cui operate, sia sulla rete di computer su cui operate, sia su qualsiasi altra applicazione che state utilizzando. Segnalare in tempo le anomalie e circostanziare gli eventi è fondamentale per prevenire problemi ben più consistenti.

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 si trasmette un virus:

- attraverso programmi provenienti da fonti non ufficiali;
- attraverso le macro di alcuni programmi;
- attraverso le email ricevute;
- attraverso il download da Internet.

Come NON si trasmette un virus:

- attraverso file di dati non in grado di contenere macro (file di testo, pdf, jpeg, ecc);
- attraverso email non contenenti allegati.

Quando il rischio da virus si fa serio:

- quando si installano programmi scaricati da internet;
- quando si copiano dati, dai dischetti;
- quando si scaricano documenti e allegati da messaggi di posta elettronica provenienti da mittenti sconosciuti;

Quali effetti ha un virus?

- Messaggi pubblicitari invadenti e persistenti, anche chiudendo i progammi o riavviando il computer;
- Nel menù appaiono funzioni extra non richieste;
- File e documenti risultano di colpo inaccessibili o introvabili;
- Le funzionalità dei computer rallentano repentinamente.
- Compaiono messaggi in lingue straniere, contenenti richieste in denaro;

Come prevenire i Virus

- **Usate 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 utilizzare programmi non autorizzati dal responsabile del trattamento dei dati.
- **Assicuratevi di non far partire accidentalmente il vostro computer da dischetto, CD o DVD**: infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.
- **Assicuratevi che il vostro software antivirus sia aggiornato**: la tempestività nell'azione di bonifica è essenziale per limitare danni che un virus può causare; inoltre è vitale che il programma antivirus sia aggiornato periodicamente (non oltre sei mesi).
- **Assicuratevi che sul vostro computer sia attivato il Firewall**: verificate dalle preferenze del vostro computer o chiedete al responsabile del trattamento dati, che sul vostro computer sia attivato il Firewall

e solo i privilegi di rete minimi necessari alle vostre esigenze d'accesso ai dati, oltretutto se sul vostro computer non vi collegate ad Internet o non inviate fax staccate il cavo telefonico per evitare possibili accessi

- **Non diffondete messaggi di provenienza dubbia:** se ricevete messaggi che avvisano di un nuovo virus pericolosissimo e che fanno riferimento ad una notizia proveniente dalla "Microsoft", ignoratelo, le email di questo tipo sono dette con terminologia anglosassone “hoax” (termine spesso tradotto in italiano con "bufala")
- **Non partecipate a "catene di S. Antonio" e simili**: analogamente, tutti i messaggi che vi invitano a "diffondete 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, per ciò utilizzare indebitamente le risorse informatiche.
- **Non aprite allegati alle email inviate da sconosciuti**: non aprite allegati alle email con file di tipo exe, zip, sit, scr, doc, xls contenenti macro e qualsiasi altro formato a voi sconosciuto se non siete certi della provenienza. Potete aprire solamente allegati di tipo pdf, jpg e file di testo che non contengono macro.

Scelta delle Password

Il più semplice metodo per l'accesso illecito ad 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 non protetto da password "poco sicura". La scelta di password "sicure" è, quindi, parte essenziale della sicurezza informatica

Cosa NON fare

- **NON dite a nessuno la vostra password.** Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.
- **NON scrivete la password da nessuna parte** che possa essere letta facilmente, soprattutto vicino al computer (es. su Post-it).
- **NON scegliete password che si possano trovare su un dizionario.** Su alcuni sistemi è possibile provare tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- **NON crediate che usare parole straniere renderà più difficile il lavorò di scoperta**, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- **NON usate il Vostro nome utente.** È la password più semplice da indovinare.
- **NON usate password che possono in qualche modo essere legate a Voi** come, ad esempio, il Vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di, telefono, ecc.

Cosa fare

- Cambiare la password a intervalli regolari. La normativa sulla privacy prevede che se sono trattati dati sensibili o giudiziari la password deve essere cambiata ogni tre mesi altrimenti ogni sei mesi. La password deve essere lunga almeno otto caratteri, meglio se con un misto di lettere, numeri e segni di interruzione.
- Utilizzate password distinte per l'accesso avari sistemi.
- Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe.

Istruzioni agli addetti al trattamento che trattano dati senza l'utilizzo di strumenti elettronici

Di seguito si riportano le misure di sicurezza idonee da adottare a cura del Responsabile e degli addetti, in caso di trattamento di dati personali senza l'ausilio di strumenti elettronici.

Modalità tecniche da adottare a cura del titolare, del responsabile e dell'addetto, in caso di trattamento con strumenti diversi da quelli elettronici:

- agli addetti sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli addetti, la lista degli addetti può essere redatta anche per classi omogenee di mansione e dei relativi profili di autorizzazione;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli addetti del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti 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;
- quando gli atti e i documenti contenenti dati personali, sensibili o giudiziari sono affidati agli addetti del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli addetti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Nell'ambito informatico il termine "sicurezza" si riferisce a tre aspetti distinti:

- **Riservatezza**: prevenzione contro l'accesso non autorizzato alle informazioni.
- **Integrità**: le informazioni non devono essere alterabili da incidenti o abusi.
- **Disponibilità**: il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi, misure soltanto tecniche, per quanto possono essere sofisticate non saranno efficienti se non usate propriamente. In particolare, le precauzioni di tipo tecnologico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessun strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

- **Utilizzare le chiavi**: il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario, non banale, per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio e riponete i documenti negli appositi contenitori alla fine di ogni giornata di lavoro.

- **Conservate i documenti in luoghi sicuri**: tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un identificativo, ma mai con i nominativi di studenti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche. Tutti i contenitori con i documenti devono essere posti in scaffalature a giorno, se poste in luoghi controllati, o armadi con serratura o ripostigli con porte con serratura se posti in luoghi noti controllati o aperti al pubblico. I dati per cui viene richiesto il blocco o la cancellazione, ma che devono essere mantenuti per un obbligo di legge o a propria tutela in quanto relativi ad adempimenti contrattuali svolti, dovranno essere posti in armadi con serratura o ripostigli con porte con serratura. I dati sensibili o giudiziari dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serratura e sono consegnati agli incaricati sotto la loro responsabilità e, al di fuori dell'orario di lavoro, solo previa registrazione I dati estremamente riservati dovranno essere posti in armadi blindati, casseforti o luoghi sicuri (locali in muratura con porta blindata). Non lasciare documenti con dati personali sui tavoli, dopo averli utilizzati, riponeteli sempre nei loro contenitori.

Zona Industriale III Fase, Viale 15 n°2 97100 Ragusa | Tel. 0932 667666 - Fax 0932667929
info@novaquadri.it | grupponovaquadri@pec.it | novaquadri.it

Istruzioni agli addetti esterni del Trattamento

Gli addetti esterni del trattamento dei dati personali, devono scrupolosamente attenersi alle seguenti istruzioni che devono essere considerate ordine di servizio.

Principi generali da osservare

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

Ai sensi dell'art.5 del Reg. UE 679/16, che prescrive i 'Principi applicabili al trattamento di dati personali" per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

I dati devono essere trattati:

- secondo il principio di **liceità**, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- secondo il principio di **trasparenza**, che consente all'interessato di venire a conoscenza delle metodologie e delle finalità di utilizzo dei propri dati;
- secondo il principio di **adeguatezza** il trattamento dei dati deve essere riferibile alla tipologia di incarico o mansione svolta;
- secondo il principio di **pertinenza,** ovvero, i dati devono essere trattati in relazione allo scopo 'cui sono destinati;
- secondo il principio della **limitatezza,** la raccolta dei dati non può eccedere ai dati strettamente necessari per la finalità perseguita.

I dati devono essere raccolti solo per **scopi**:

- **esatti**, cioè, precisi e rispondenti al vero e se necessario, **aggiornati**
- **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i. tempi di conservazione degli atti amministrativi. Trascorso, detto periodo i dati vanno resi anonimi o cancellati la loro comunicazione diffusione non è più consentita.
- Trattati in modo tale che venga garantita un'adeguata sicurezza dei dati personali mediante misure tecniche ed organizzative adeguate;
- **determinat**i, vale a dire che non è consentita la raccolta come attività fine a sé stessa;
- **espliciti,** nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- **legittimi**, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

In particolare, i dati idonei a rivelare lo **stato di salute** o la **vita sessuale** sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di **riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Ciascun Addetto deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni di cui al Regolamento Europeo in materia di trattamento dei dati personali sono previste **sanzioni amministrative** e **pecuniarie** (art. 83). Per le altre sanzioni riferibili alle violazioni non soggette amministrative e pecuniarie si rimanda alla legislazione nazionale.

In ogni caso, la responsabilità penale per eventuale uso non corretto dei dati oggetto di tutela resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

Mentre, in merito alla responsabilità civile, si fa rinvio all'art.2050 del Codice civile, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornite prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

Compiti particolari dell'addetto esterno

L'addetto esterno al trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare:**

- identificare e censire i **trattamenti** di dati personali, le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- definire, per ciascun trattamento di dati personali, **la durata** del trattamento e la **cancellazione** o trasformazione in forma anonima dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita **l'informativa** ai soggetti interessati, ai sensi dell'artt.13 – 14 –21del Regolamento;
- adempiere agli **obblighi di sicurezza**, quali attenersi alle disposizioni di cui agli artt.25 e 32 del Regolamento, cioè adottare le misure di sicurezza idonee adottare tutte le **preventive misure di Sicurezza** ritenute **idonee** al fine di ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- **comunicare** tempestivamente al Titolare casi di **accesso non autorizzato** ai dati o di trattamento non consentito o non conforme alle finalità perseguite;
- far osservare gli adempimenti previsti in caso di **nuovi trattamenti e cancellazione** di trattamenti;
- segnalare al Responsabile l'eventuale cessazione di trattamento.

In merito agli addetti, l'addetto esterno deve:

- individuare, trai propri collaboratori, designandoli per iscritto, addetti al trattamento fornendo loro le **istruzioni** a cui devono attenersi per svolgere le operazioni di trattamento;
- **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli addetti del trattamento, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati e l'osservanza parte degli addetti, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
- stabilire le modalità di **accesso** ai dati e l'organizzazione del lavoro degli addetti, avendo cura di adottare preventivamente le misure organizzative idonee e impartite le necessarie istruzioni ai fini di riscontro di eventuali richieste di esecuzione dei diritti di cui all'art.5, agli artt. 12 e ss. Fino al 22 e all'art. 34;
- evadere le eventuali richieste di accesso, rettifica, integrazione, cancellazione, blocco dei dati da parte dell'interessato che eserciti i propri diritti ai sensi degli artt. di cui sopra;
- collaborare con Ogni Titolare all'adempimento e all'adempimento degli obblighi previsti dal Regolamento e segnalare eventuali problemi applicativi.

Istruzioni al/ai Responsabile/i del Trattamento

Il Responsabile del trattamento è debitamente nominato dal Titolare del trattamento in osservanza alle disposizioni dell'art.28.

Il responsabile del trattamento dei dati personali deve scrupolosamente attenersi alle seguenti istruzioni che devono essere considerate ordine di servizio.

Principi generali da osservare

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale. Ai sensi dell'art.5 del Reg. UE 679/16, che prescrive i "Principi applicabili al trattamento di dati personali" per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

I dati devono essere trattati:

- secondo il principio di **liceità**, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- secondo il principio di **trasparenza**, che consente all'interessato di venire a conoscenza delle metodologie e delle finalità di utilizzo dei propri dati;
- secondo il principio di **adeguatezza** il trattamento dei dati deve essere riferibile alla tipologia di incarico o mansione svolta;
- secondo il principio di **pertinenza,** ovvero, i dati devono essere trattati in relazione allo scopo 'cui sono destinati;
- secondo il principio della **limitatezza,** la raccolta dei dati non può eccedere ai dati strettamente necessari per la finalità perseguita.

I dati devono essere raccolti solo per **scopi**:

- **esatti**, cioè, precisi e rispondenti al vero e, se necessario, **aggiornati**
- **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i. tempi di conservazione degli atti amministrativi. Trascorso, detto periodo i dati vanno resi anonimi o cancellati la loro comunicazione diffusione non è più consentita.
- Trattati in modo tale che venga garantita un'adeguata sicurezza dei dati personali mediante misure tecniche ed organizzative adeguate;
- **determinat**i, vale a dire che non è consentita la raccolta come attività fine a sé stessa;
- **espliciti,** nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- **legittimi**, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

In particolare, i dati idonei a rivelare lo **stato di salute** o la **vita sessuale** sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di **riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Ciascun addetto deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni di cui al Regolamento Europeo in materia di trattamento dei dati personali sono previste **sanzioni amministrative e pecuniarie** (art. 83). Per le altre sanzioni riferibili alle violazioni non soggette amministrative e pecuniarie si rimanda alla legislazione nazionale.

In ogni caso, **la responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

Zona Industriale III Fase, Viale 15 n°2 97100 Ragusa | Tel. 0932 667666 - Fax 0932667929
info@novaquadri.it | grupponovaquadri@pec.it | novaquadri.it

Mentre, in merito **alla responsabilità civile**, si fa rinvio all'art.2050 del Codice Civile, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che per evitare ogni responsabilità, l'operatore è tenuto a fornire prava di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

Compiti particolari dell'addetto esterno

L'addetto esterno al trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare:**

- identificare e censire i **trattamenti** di dati personali, le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- definire, per ciascun trattamento di dati personali, **la durata** del trattamento e la **cancellazione** o trasformazione in forma anonima dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita **l'informativa** ai soggetti interessati, ai sensi dell'artt.13 – 14 –21del Regolamento;
- adempiere agli **obblighi di sicurezza**, quali attenersi alle disposizioni di cui agli artt.25 e 32 del Regolamento, cioè adottare le misure di sicurezza idonee adottare tutte le **preventive misure di Sicurezza** ritenute **idonee** al fine di ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- **comunicare** tempestivamente al Titolare casi di **accesso non autorizzato** ai dati o di trattamento non consentito o non conforme alle finalità perseguite;
- far osservare gli adempimenti previsti in caso di **nuovi trattamenti e cancellazione** di trattamenti;
- segnalare al Titolare l'eventuale cessazione di trattamento.

In merito agli addetti, l'addetto esterno deve:

- individuare, trai propri collaboratori, designandoli per iscritto, addetti al trattamento fornendo loro le **istruzioni** a cui devono attenersi per svolgere le operazioni di trattamento;
- **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli addetti del trattamento, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati e l'osservanza parte degli addetti, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
- stabilire le modalità di **accesso** ai dati e l'organizzazione del lavoro degli addetti, avendo cura di adottare preventivamente le misure organizzative idonee e impartite le necessarie istruzioni ai fini di riscontro di eventuali richieste di esecuzione dei diritti di cui all'art.5, agli artt. 12 e ss. Fino al 22 e all'art. 34;
- evadere le eventuali richieste di accesso, rettifica, integrazione, cancellazione, blocco dei dati da parte dell'interessato che eserciti i propri diritti ai sensi degli artt. di cui sopra;
- collaborare con Ogni Titolare all'adempimento e all'adempimento degli obblighi previsti dal Regolamento e segnalare eventuali problemi applicativi.

Piano Formativo

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

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Verifica formazione personale	Tutti gli incaricati al trattamento	6 mesi

In osservanza alle disposizioni dell'art. 28 e art. 32 comma 4 del Reg. EU 679/16, tutti i soggetti addetti al trattamento dei dati personali devono essere in grado di fornire al Titolare garanzie professionali sufficienti che soddisfino i requisiti di formazione e competenza richiesti dalla natura dell'incarico. A tal proposito gli interventi formativi rivolti agli addetti dei trattamenti hanno la finalità di rendere loro edotti:

1. sulla segretezza della componente riservata della credenziale e sulla diligente custodia dei dispositivi in possesso ed uso esclusivo dell'addetto;
2. sulla custodia e l'accessibilità dello strumento elettronico durante una sessione di trattamento;
3. sul controllo e sulla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
4. sul controllo e sulla custodia degli atti e i documenti contenenti dati personali sensibili o giudiziari a loro affidati per lo svolgimento dei relativi compiti fino alla restituzione al termine delle operazioni in maniera che ad essi non accedano persone prive di autorizzazione;
5. sulle procedure istituzionali da applicare per la sicurezza e la protezione dei dati, quali ad esempio il cambio delle password, il salvataggio dei dati, aggiornamenti di antivirus e tutto quanto necessario a far si che le misure di sicurezza reputate idonee Titolare vengano a tutti gli effetti messe in pratica;
6. sui profili di autorizzazione e gli ambiti di applicazione degli stessi riferiti per classi omogenee di addetti;
7. sulle Policy istituzionali in riferimento all'utilizzo della posta elettronica ed internet, sul sistema di videosorveglianza e sull'Amministratore di sistema qualora la struttura ne necessiti;
8. sui diritti dell'interessato ex artt. dal 15 al 22.

Il piano formativo del personale viene inoltre redatto tenendo conto dei seguenti criteri:

a) aggiornamento sistematico delle istruzioni agli addetti;
b) verifica costante delle istruzioni impartite agli addetti;
c) aggiornamento periodico sulle misure di sicurezza adottate.

Piano di Emergenza

Nell'ottica dell'importanza della circolazione dei dati e della correlata necessità di gestirne il flusso e il lecito trattamento, bisogna provvedere a porre in essere azioni al seguito del verificarsi, di eventuali eventi dannosi o pericolosi per il trattamento dei dati personali.

In relazione alle misure di sicurezza predisposte Ogni Titolare ha predisposto un quadro delle possibili intromissioni o effrazioni ai sistemi informatici (attacco di un virus, hacking, furto dati, errore umano) alle quali ha associato le relative azioni correttive.

1. Nel caso di accessi non autorizzati verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tinte le connessioni con Internet;

   Verrà controllata tutta la rete dei computer, tutti i sistemi operativi, tutti i software installati e tutti i dati inseriti per verificare eventuali danni provocati dagli accessi non autorizzati e per il ripristino della normalità.

2. Nel caso l'accesso non autorizzato sia stato effettuato per scopi fraudolenti o di sabotaggio si provvederà all'immediata denuncia pressò le forze di polizia e/o l'autorità giudiziaria dell'eventuale responsabile degli accessi non autorizzati.
3. Nel caso l'accesso non autorizzato sia stato effettuato con scopi non conformi alle norme interne della nostra organizzazione ma comunque non a scopo fraudolento o di sabotaggio verranno adottati tutti i provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.

In ogni caso per ognuna delle situazioni sopra citate o comunque per tutte le violazioni dei dati si provvederà a dare tempestiva comunicazione all'autorità garante come procedura prevista nel modulo in allegato.

Per accesso non autorizzato si intende:

- l'accesso effettuato da un operatore non autenticato utilizzando le credenziali di autenticazione di un addetto
- l'accesso effettuato aggirando il sistema di autenticazione
- l'accesso effettuato da un addetto autenticato in aree non previste dal sistema di autorizzazioni
- l'accesso tramite intercettazioni di informazioni in rete
- l'accesso non autorizzato a locali/aree ad accesso non riservato
- l'accesso a strumenti contenenti dati che sono stati sottratti.

4. Nel caso di comportamenti sleali e fraudolenti degli addetti sarà bloccato immediatamente l'accesso ai dati degli addetti e adottati i relativi provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.
5. Nel caso di azione di virus informatici verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete attraverso l'utilizzo di un programma antivirus aggiornato e verrà immediatamente verificata e bonificata tutta la rete dei computer.
6. Nel caso di spamming verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tutte le connessioni con Internet, verificherà i firewall su ogni computer e l'aggiornamento periodico dei programmi antivirus su ogni computer e tutta la rete dei computer.
7. Nel caso di azione dei programmi suscettibili di recare danno verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà i programmi dannosi e verrà immediatamente verificata e bonificata tutta la rete dei computer.

Valutando le criticità emerse dalla valutazione dei rischi si può considerare il livello di rischio come MEDIO-BASSO constatandosi un elevato livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati.

Il Piano di emergenza elaborato di cui sopra si riferisce a quelle azioni negati forti come elencate precedentemente.

In relazione a quegli eventi dannosi che comportano: un elevato livello di criticità per il dato personale stesso, Ogni Titolare ha previsto un tempo di ripristino pari a 7 giorni per i seguenti casi di violazioni illecite o accidentali di dati:

- Perdita
- Distruzione
- Modifica
- Divulgazione non autorizzata
- Accesso ai dati personali che siano trasmessi, conservati o trattati

Al fine di ripristinare gli archivi e dati, si è provveduto a conservare in un luogo esterno alla sede, copie aggiornate settimanalmente sia dei dati che dei software (applicativi e sistemi operativi).

In aggiunta a ciò, il fornitore delOgni Titolare garantisce la consegna di strumenti elettronici con la stessa configurazione entro tre giorni dall'avvenuta violazione, considerando il tempo minimo di un giorno per l'installazione del sistema operativo e dei software applicativi.

Il trattamento di tutti i dati processati sarà ripristinato entro i 7 giorni del termine di cui sopra.

Nella definizione del piano di emergenza, Ogni Titolare ha predisposto eventi formativi per tutti gli incaricati e i responsabili del trattamento dati nell'ottica di definite le azioni consentite e quelle non consentite agli stessi soggetti interessati. Nello stesso ambito ha fornito dovuta e comprovata formazione dei possibili eventi negativi e delle relative azioni correttive da porre in essere, in modo tale da rendere note agli addetti ed ai responsabili del trattamento le procedure da attivare per risolvere oi contenere l'effetto negativo scaturito dall'evento dannosa.

Responsabili o consulenti e autorità da contattare in caso di emergenza

Ogni Titolare del Trattamento a norma dell'art. 33 del Regolamento, qualora la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, è tenuto ad effettuare senza ingiustificato ritardo, entro massimo le 72 ore dal momento in cui ne è venuto a conoscenza, la notificazione presso l'autorità competente, di cui all'art.55, della avvenuta violazione. L'attività può essere supportata dal Responsabile per la Protezione dei Dati.

Nel caso di violazione che comporti un rischio consistente per i diritti e le libertà delle persone fisiche la comunicazione va fatta all'autorità competente e contestualmente all'interessato come dispone l'art.34.

Ogni Titolare si fa carico di adottare tutte le misure idonee a prevenire o risolvere eventuali eventi dannosi e di comunicare tempestivamente ogni violazione avvenuta presso l'autorità competente a norma dell'art. 83.