# MODELLO ORGANIZZATIVO PRIVACY 3G
# 3G S.p.A.

**Il presente DOCUMENTO è stato emesso in data 15 Maggio 2018 ed è stato aggiornato periodicamente sino alla data del 15 giugno 2020**

**E' STATO REDATTO AI SENSI E PER GLI EFFETTI DEL Nuovo Regolamento Europeo n. 2016/679 e del Decreto Legislativo 10 agosto 2018, n.101**

**3g SpA** - Sede legale: Via Crescenzio, 9 - 00193 Roma - Telefono: 06 95229300 - Fax: 06 92912897
C.F./P.Iva 02619020122 - Registro delle Imprese di Roma Rea n. 1067663 - Capitale sociale Euro 400.000,00
Sedi operative:
Sulmona Viale del Lavoro, 2 - 67039 (AQ) - Telefono: 0864 251924 - Fax: 0864 33781
Campobasso Via San Lorenzo, 64 - 86100 (CB) - Telefono: 0874 1960800 - Fax: 0874 484324
Chieti Scalo Via Padre Ugo Frasca, snc - 1°piano scala B c/o Centro DA.MA - 66100 (CH) - Telefono: 0871 5481 - Fax 0871 923113

Scopo di questo documento è delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate o da adottare per la tutela dei dati personali affinché siano rispettati gli obblighi previsti dalle Leggi vigenti; analizzare i rischi generici rispetto alla protezione dei dati personali trattati nell'ambito dell'attività operativa e di staff di 3g S.p.A. e dei suoi fornitori, Committenti, Collaboratori esterni.

Destinatari del documento sono:

- Personale 3g S.p.A.;
- Fornitori;
- Committenti;
- Enti ed Autorità in attività ispettiva.

Il presente documento è valido fino al **31 Dicembre 2020** si procederà al solo aggiornamento delle informazioni qualora le stesse per motivi diversi non risultassero più coerenti con l'organizzazione o con il trattamento dei dati.

Al presente piano privacy generale e valutazione di impatto generale, si affiancano e si affiancheranno nel tempo specifiche valutazioni di impatto effettuate per singola commessa. Da esse scaturiranno le misure da affiancare ai piani privacy indicati di volta in volta dal Committente\Titolare dei dati.

**Tipologia di dati trattati**: rinvio a registri dei trattamenti e, ove presenti, a valutazioni di impatto generale e per singola commessa.

## ORGANIGRAMMA PRIVACY

Ferma restando la figura dell'Amministratore Unico nel ruolo di Responsabile ESTERNO del trattamento dei dati personali ex art. 28 GDPR nominato dai Committenti nonché di Titolare dei dati personali interni, il modello organizzativo di 3g S.p.A. prevede, attualmente, la coesistenza delle seguenti figure, nominate in ottemperanza al sistema integrato di Protezione del Dato denominato "Progetto Privacy 3g":

A) **Consulente Privacy stabile in outsourcing**: Area Legale S.r.l.s. mette a disposizione di 3g S.p.A. un Legale specializzato che coadiuva il Legale Interno e la Struttura rispetto all'impostazione del presente Piano Privacy Aziendale e dei Piani Privacy di Commessa (che valutano la qualità e la tipologia dei dati in entrata rispetto alla specifica commessa e indicano le misure da applicare). Al Consulente, al Referente Privacy Inetrno (vedi infra) ed al Data Protection Officer è demandata la formazione del personale 3g sul tema privacy, tutta assistita da test pre e post

sessione e debitamente registrata in apposito registro così articolata:

- **formazione di primo livello: trimestrale**

tale formazione, di alto standing, entra nel merito della normativa vigente ed è volta ad assicurare la massima comprensione delle procedure e delle policy aziendali sul tema, nonché a raccogliere indicazioni e suggerimenti dal basso onde integrare e migliorare i Piani Privacy che dettano queste ultime;

- **formazione di secondo livello: semestrale**

mirata a rendere il personale edotto rispetto al contenuto dei Piani Privacy, Aziendale e di Commessa, analizzare casi pratici e verificare il corretto adempimento della policy privacy e della normativa;

- **formazione di terzo livello: in forma orale + scritta + formazione visive**

La prima della durata di 45 minuti a cura del Referente Privacy interno ed erogata a tutto il personale (dipendenti e collaboratori) al primo contratto viene richiamata trimestralmente a mezzo test online per verificare la tenuta formativa; la seconda, a livello di informative recettizia, divulgata mediante circolare consegnata al lavoratore al momento dell'assunzione e attraverso aggiornamenti periodici, pone il personale a conoscenza delle policy privacy aziendali on the job e delle procedure da porre in essere in caso di criticità (es. Data Breach). La terza (cartellonistica esplicativa in tutte le sale di produzione e nelle aree comuni + newsletter a mezzo email + pillole video a mezzo email), mira a tenere viva l'attenzione al tema della protezione dei dati e a fornire indicazioni immediate e chiare (es. "cosa fare in caso di sospetta violazione dei dati") nonché sensibilizzare in modo continuo il personale;

B) **Referente Privacy tecnico-giuridico/Comitato Privacy tecnico**:

Tale struttura, è composta da 6 membri, tutti altamente e costantemente formati in materia di protezione dei dati personali e, specificatamente, da un coordinatore (ex responsabile ufficio privacy) + 5 elementi provenienti dalle aree HR (1), Legal (1), IT (1), Produzione (1), Ufficio Gare\Bandi (1). Il Data Protection Officer è presente su invito del coordinatore e, comunque, in pianta stabile per tutta la durata dell'emergenza.

Il Comitato si dedica altresì allo studio ed alla divulgazione delle ISTRUZIONI FORNITE dai singoli Titolari (Committenti) rispetto alla protezione dei dati, facendo in modo che le stesse vengano recepite ed applicate dall'intera struttura interessata dal trattamento.

Il Comitato si riunisce con cadenza settimanale, individua le misure da mettere in campo e monitora l'efficacia di quelle già in essere, verbalizzando di volta in volta.

Provvede all'analisi dei flussi dei dati tra tutte le funzioni aziendali e verso l'esterno; verifica, aggiornamento, revisione e stesura di tutta la documentazione privacy (informative, registro trattamenti, etc); coordinamento e stesura Valutazione dei Rischi; coordinamento e stesura Valutazione di Impatto; stesura e revisione di tutti i documenti afferenti la privacy; analisi dei contratti con Clienti e verifica delle incombenze privacy con

eventuale suggerimento di ulteriori misure; analisi di tutti i contratti con i Fornitori; presenzia e coordina le risposte del Comitato tecnico agli Audit esterni; programma e coordina gli Audit ai Responsabili Esterni; gestisce,coordina, stila le relazioni del Comitato tecnico al Comitato decisionale in via ordinaria e in caso di violazione dei dati; proposizione e studio di misure di mitigazione rispetto ai trattamenti e ai flussi di tutte le funzioni aziendali e verso l'esterno; formazione al personale in materia di protezione dei dati personali; conservazione di tutta la documentazione secondo il principio dell'accountability; ogni altra attività relativa ai dati personali.

C) **Amministratore di sistema:**

garantisce l'applicazione delle misure di protezione previste dai Piani Privacy (Aziendale e di Commessa) sui servers e sugli strumenti informatici; è responsabile della definizione, dell'implementazione e della manutenzione dei dispositivi e delle tecnologie di sicurezza che costituiscono la rete Aziendale nonché dell'organizzazione dell'Information Security Management System (ISMS);

D) **Responsabili Esterni del Trattamento dei dati personali ex art. 28 GDPR:**

nominati formalmente con contratto che prevede l' allegazione e l'accettazione delledi policy aziendali in tema protezione dei dati personali nella persona di tutti i consulenti esterni, dei subappaltatori-subagenti, dei fornitori, dei committenti ove trattino dati di personale 3g S.p.A. (es. gestione ed emissione credenziali di accesso a piattaforme software del committente).

E) **Preposti alla verifica del corretto adempimento degli oneri privacy:**

sono i diretti responsabili, nei confronti del Titolare, della verifica dell'effettivo rispetto della normativa Privacy e della applicazione dei Piani Privacy (Aziendale e di Commessa). Sono stati formalmente nominati tutti i top manager, i responsabili di ufficio, di produzione, di stabilimento, di funzione, di commessa sino al livello Team Leader. Beneficiano di formazione di primo (responsabili di funzione, stabilimento, top management) e di secondo livello (responsabili di commessa e team leaders);

F) **Incaricati\autorizzati del Trattamento**:

nominati dall'Amministratore Unico, vengono resi edotti mediante la formazione di cui sopra e le circolari, delle policy privacy da rispettare e delle modalità di segnalazione di eventuali anomalie, nonché delle eventuali conseguenze in caso di mancato rispetto delle procedure;

G) **Responsabile per la protezione dei dati (Data Protection Officer)**.

Il DPO è un soggetto dotato di piena autonomia ed indipendenza nello svolgimento dei propri compiti. Egli risponderà solo ed esclusivamente nei confronti del Titolare del trattamento o del Responsabile del trattamento da cui è stato nominato. Ha il compito di vigilare sull'osservanza del Regolamento UE 2016/679 e, più in generale, della normativa vigente in materia di privacy. Egli deve informare il Titolare del trattamento in merito agli obblighi del Regolamento UE 2016/679 e dalla normativa vigentei in materia di privacy.

Deve inoltre supportare il Titolare in ogni attività di trattamento dei dati (Registro dei dati del trattamento, Data Protection Impact Assessments (DPIA), procedure di Data Breach). Il DPO ha il compito di cooperare con l'Autorità Garante in materia di protezione dei dati personali e fungere da elemento di contatto fra questa ed il Titolare del trattamento;
Inoltre dev'essere consultato in caso di data breach ed assistere il Titolare del trattamento in caso di necessità di notifica al Garante.

H) **Certificazioni:** In data 30 ottobre 2018 è stata acquisita certificazione **ISO 27001 (Allegato)**
Si sta procedendo a mettere 3g S.p.A. in linea con lo Schema **ISDP 1003:2008**

**Sulla base della quantità e della qualità dei dati trattati, è stata quindi elaborata e divulgata la seguente:**

## POLICY AZIENDALE PER LA PROTEZIONE DEI DATI PERSONALI

### Istruzioni generali per tutti gli incaricati al trattamento

Al fine di meglio attuare le previsioni di Legge, in chiave di un capillare monitoraggio e formazione rispetto alla protezione dei dati, nonché ad integrazione di quanto previsto nel contratto Collettivo di categoria e nel Contratto individuale di lavoro, tutti i dipendenti e i collaboratori sono nominati Incaricati del trattamento.
Gli Incaricati del trattamento sono chiamati ad operare sotto la diretta autorità e controllo del Titolare e/o del Responsabile Esterno al trattamento della competente Direzione 3G, attenendosi alle istruzioni impartite in merito al trattamento dei dati personali al fine di adempiere agli obblighi previsti dal Regolamento Privacy, effettuato mediante l'utilizzo di mezzi elettronici e/o automatizzati.
I dati personali cui gli Incaricati del trattamento sono autorizzati ad accedere sono i soli la cui conoscenza è strettamente necessaria per adempiere i compiti assegnati.
Gli Incaricati dovranno trattarli esclusivamente per fini aziendali e secondo le specifiche istruzioni e previste dalla normativa privacy e che saranno stabilite dal Titolare con il supporto del PREPOSTO che segnalerà, per l'Unità Operativa/Ufficio/Area da egli coordinata/diretta, le misure peculiari che ritiene essenziali o utili rispetto al tipo di trattamento effettuato ed al tipo di dati trattati.
Alla luce di quanto sopra esposto i soggetti nominati incaricati del trattamento sono tenuti, anche in base a quanto stabilito dal codice privacy, a:

- operare con metodologie e strumenti di lavoro idonei alla acquisizione esatta dei dati, all'eventuale loro aggiornamento e conservazione in ogni fase di trattamento;
- trattare i dati personali garantendo la massima riservatezza delle informazioni di cui vengono in possesso;
- evitare che i dati siano soggetti a rischi di perdita o distruzione anche accidentale;
- evitare che ai dati possano accedere persone non autorizzate;
- evitare che vengano svolte operazioni di trattamento non consentite o non conformi

ai fini per i quali i dati sono stati raccolti e per i quali vengono trattati;

- non eseguire operazioni per fini non previsti tra i compiti assegnati e non svolgere alcuna attività che non sia espressamente ricompresa nel proprio profilo di abilitazione;
- non utilizzare dispositivi fotografici nelle sale di lavoro, non effettuare “screenshots” di alcun tipo, non utilizzare supporti magnetici;
- curare l’attivazione del salvaschermo durante il momentaneo utilizzo del terminale p.c.;
- curare la segretezza della password di accesso al p.c. assegnata;
- trattare e custodire i dati stessi con diligenza, evitando azioni che possano far conoscere a persone non incaricate i dati stessi. In particolare, per i trattamenti dei dati personali che dovessero comportare l’uso di sistemi informatici e telematici, l’accesso a tali dati da parte degli Incaricati potrà avvenire solo attraverso password o codici di accesso secondo i criteri e le modalità impartite dal Titolare sulla base del Titolo V° – Capo I°- e dell’Allegato B del Codice sulle misure minime di sicurezza. Nessun dato personale, su supporto magnetico o digitale, potrà in ogni modo essere lasciato incustodito e trasportato al di fuori delle aree di lavoro in cui avvengono i trattamenti;
- custodire con pari diligenza tutto il materiale cartaceo relativo ai dati personali. Tale materiale non potrà essere lasciato incustodito sulle scrivanie e, a fine lavoro, dovrà essere riposto in armadi o cassetti chiusi a chiave. Durante le normali quotidiane operazioni di lavoro, non dovrà risultare visibile a persone non incaricate del trattamento (es. personale addetto alle pulizie o manutenzione o vigilanza);
- evitare di divulgare informazioni o dati acquisiti per errore (es. mail ricevuta erroneamente contenenti dati personali di cui il ricevente non è titolare o rinvenimento di materiale cartaceo o supporti informatici) ma darne immediato avviso secondo le modalità di cui al punto seguente;
- seguire, in caso di rinvenimento di una qualunque violazione di dati personali (“Data breach”), la seguente procedura:

informare immediatamente, verbalmente e riservatamente il proprio superiore in linea gerarchica e far seguire a stretto giro (entro e non oltre minuti 15) e-mail, sempre a proprio superiore gerarchico, riportante la segnalazione e accurata descrizione della situazione, mettendo in copia, altresì, l’indirizzo: **ufficioprivacy@3gspa.net** ed al preposto alla verifica della applicazione delle policy in tema privacy, individuato nel Responsabile della Sua Unità Operativa/Ufficio/Area, mettendo come oggetto: **possibile DATA BREACH**;

## Misure generali adottate all’interno della struttura 3g S.p.a.

### Misure di protezione fisica e gestione documenti cartacei

- Anonimizzazione di tutti i documenti da scambiare in forma di “format”;
- Segregazione dei documenti contenenti dati ex art. 9 GDPR o ex sensibili all’interno di cartelline separate negli schedari;
- Utilizzo di schedari chiusi con chiave in possesso dei soli soggetti titolati a trattare i dati ivi contenuti;
- Abilitazione all’utilizzo delle fotocopiatrici a mezzo codice personale;
- Accesso agli stabilimenti limitato a mezzo tornelli e badges;

- Accesso alle sale operative limitato a mezzo badge
- Uffici chiusi a chiave ove non presidiati;
- Chiavi di accesso agli uffici conservate in armadietti chiusi a chiave e chiave assegnata nominalmente;
- Sistema di sorveglianza private degli stabilimenti e Sistema di allarme;
- Sistema antincendio a norma;
- Informative ex. Capo III GDPR allegate a contratti, disponibili su sito web, erogate in sede di selezione e recruiting;
- Servers ubicati in ServerFarm di tipo Tier IVe backup in due diverse località distanti oltre 500 km l'una dall'altra. Si prevede il passaggio a Cloud entro il 2020 ;
- Disabilitazione di tutti gli accessi USB dalle postazione di lavoro;

**Misure di protezione dati in forma digitale e Trattamenti di dati personali effettuati con l'ausilio di strumenti elettronici**

**Autenticazione**

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di **credenziali di autenticazione** (l'insieme degli strumenti elettronici, dei software e delle procedure atte a verificarne l'identità) che consentano il superamento di una procedura di autenticazione.

Le credenziali di autenticazione (i dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica) consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo; ad ogni incaricato è assegnata individualmente una credenziale per l'autenticazione e nelle istruzioni impartite a ciascuno al momento dell'assunzione dell'incarico è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per la protezione dei dati ed il suo corretto utilizzo è prima di tutto a garanzia dell'utente. La parola chiave prevista dal sistema di autenticazione è composta da almeno otto caratteri; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. Non viene comunicata ad alcuno per alcun motivo, e non viene conservata annotazione scritta in alcun posto, specie nei pressi della postazione di lavoro.

Il codice per l'identificazione non viene assegnato ad altri incaricati, neppure in tempi diversi.

Si provvede alla tempestiva disattivazione del codice per l'identificazione nel caso in cui non venga utilizzato per almeno sei mesi (salvo che si tratti di credenziali di autenticazione preventivamente autorizzate per soli scopi di gestione tecnica). Le credenziali sono prontamente disattivate anche in caso di perdita della qualità che consente all'incaricato

l'accesso ai dati personali.

Sono impartite idonee istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Se si allontana dalla propria postazione l'incaricato dovrà mettere in protezione il suo sistema (Pc client o portatile) affinché persone non autorizzate non abbiano accesso ai dati protetti.

Sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o
impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del Sistema.

Essendo per gli incaricati individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

- AGGIORNAMENTO PERIODICO DELL'INDIVIDUAZIONE DELL'AMBITO DEL TRATTAMENTO CONSENTITO AI SINGOLI INCARICATI E ADDETTI ALLA GESTIONE O ALLA MANUTENZIONE DEGLI STRUMENTI ELETTRONICI

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione relativi ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.

- PROTEZIONE DEGLI STRUMENTI ELETTRONICI E DEI DATI RISPETTO A TRATTAMENTI ILLECITO DI DATI, AD ACCESSI NON CONSENTITI E A DETERMINATI PROGRAMMI INFORMATICI

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale mediante l'attivazione di idonei strumenti elettronici che vengono aggiornati con cadenza almeno semestrale. Ogni gateway - l'insieme di hardware, software e applicazioni che permettono l'interconnessione (Internet) o l'accesso remoto a sistemi esterni - deve essere protetto. I Gateway devono consentire l'accesso alla rete interna solamente agli utenti autorizzati attraverso sistemi di controllo specifici (Proxy/Firewall).
A tale scopo per tutte le postazioni che sono collegate verso internet è necessario predisporre un sistema che impedisca accessi indesiderati.

Tali sistemi, denominati "Firewall", servono a prevenire l'accesso da parte di "intrusi" ai sistemi di gestione dati e devono disporne tutti i sistemi attraverso il server dati (se è quest'ultimo a consentire la connessione all'esterno) o direttamente ogni singola postazione, se ciascuna si connette ad internet con un modem. Ogni trimestre è necessario verificare se sono disponibili degli aggiornamenti sul Firewall.

Le postazioni che ricevono le mail direttamente dall'esterno dispongono di un Antivirus in grado di controllare le mail in arrivo e quelle in partenza. In caso di segnali allarmanti (mail sospette, comportamenti della cpu imprevedibili) si verifica immediatamente l'efficienza dell'antivirus ed il suo stato di aggiornamento. Semestralmente si procede a verificare che tutti i programmi antivirus si siano correttamente aggiornati. In caso di mancato aggiornamento del software antivirus si provvede a ripristinarne immediatamente il funzionamento. La responsabilità dell'efficacia di tale sistema è assegnata al responsabile dei servizi informativi. Le istruzioni riguardanti l'utilizzo del sistema antivirus e del relativo aggiornamento sono riportate nelle guide operative del prodotto (**attualmente Karspersy**). Annualmente si provvede all'effettuazione degli aggiornamenti (patch) dei programmi per elaboratore volti a prevenire le vulnerabilità (bug) di strumenti elettronici e a correggerne i difetti.

Il Titolare del trattamento adotta misure minime di sicurezza avvalendosi altresì di soggetti esterni alla propria struttura che garantiscono i criteri di affidabilità richiesti dal GDPR e dalla policy interna. **Attualmente 3g Innovation Technology S.r.l.**
Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza giornaliera. Le copie di sicurezza vengono effettuate automaticamente, previa immissione della password, su server di backup; ogni copia di sicurezza, etichettata per tipo di database e data di salvataggio, viene opportunamente segregata in luogo diverso da quello di elaborazione.
Annualmente vengono testate le procedure di ripristino, che prevedono il ripristino in linea dei dati, l'esecuzione delle procedure eseguito da parte del personale specializzato.

## Direttive di gestione delle credenziali di accesso alla postazione di lavoro (vedasi Allegato)

## Distribuzione dei compiti e delle Responsabilità alla data di aggiornamento del presente documento

**Il Titolare del trattamento dei dati ha conferito, con lettera allegata in copia alla presente relazione, la mansione di PREPOSTI alla verifica del corretto adempimento delle policy privacy e della normativa vigente ai seguenti soggetti**

*Omissis*

**Il Titolare del trattamento dei dati conferisce con lettera allegata in copia alla presente relazione la nomina di RESPONSABILI ESTERNI DEL TRATTAMENTO EX ART. 28 GDPR AI SEGUENTI SOGGETTI:**

*Omissis*

**Il Titolare del trattamento dei dati ha conferito, con lettera allegata in copia alla presente relazione, la mansione di AMMINISTRATORE DI SISTEMA ai seguenti soggetti:**

*Omissis*

**Il Titolare del trattamento dei dati ha constituito con lettera allegata in copia alla presente relazione il COMITATO PRIVACY TECNICO (Privacy Team) che è composto da:**

*Omissis*

**Il Titolare del trattamento dei dati ha conferito l'incarico di Responsabile della protezione dei dati personali (Data Protection Officer) al seguente soggetto:**

- Avv. Sergio Aracu

Oltre ai sopra indicati soggetti, in chiave di approccio proattivo alla compliance GDPR, 3g S.p.A. ha ritenuto opportuno provvedere alla formalizzazione della nomina ad incaricato a tutti coloro che sono addetti al compimento delle operazioni di trattamento di dati personali, anche di natura sensibile. In tal modo si ritiene di agire utilmente rispetto alla sensibilizzazione ed alla chiarezza in chiave di protezione dei dati personali.
Sono pertanto stati nominati **INCARICATI al trattamento dei dati personali** tutti gli **OPERATORI ed il personale di staff,** che per semplicità sono stati ricompresi in un'unica classe omogenea di attività;

## Ulteriori misure di protezione

Sono state predisposte idonee procedure di accesso e di protezione della SALA SERVER, in considerazione della specifica criticità che tali locali possono avere nella gestione globale dei trattamenti di dati personali. A tale scopo, l'accesso alla sala server è consentito solo alla persona incaricata della manutenzione per il compimento delle necessarie operazioni nell'area, ed è prevista la preventiva identificazione, autorizzazione e registrazione di tutti coloro che, a vario titolo, hanno la necessità di accedere alle aree predette.

La procedura per il reimpiego di strumenti e supporti informatizzati prevede che nessun supporto informatizzato contenente dati personali possa essere rimosso dalla sede in cui è stato utilizzato, se prima non sono stati eliminati i dati stessi. Fa eccezione il trasporto dei supporti informatici generati nelle procedure di salvataggio ad un eventuale altro sito noto, per motivi di disaster recovery, da parte di personale incaricato dal Titolare del trattamento dei dati/Responsabile Esterno del Trattamento. Il riutilizzo dei supporti informatizzati è inibito se cambiano le finalità e le modalità del trattamento.
Quando non più adoperati, si provvede a distruggere o a rendere inutilizzabili i supporti rimovibili su cui sono memorizzati dati sensibili o giudiziari, e si consente il loro riutilizzo da parte di altri incaricati non in possesso di idonea autorizzazione al trattamento degli stessi dati solo a condizione che le informazioni precedentemente in essi contenute siano state rese non più intelligibili e tecnicamente in alcun modo ricostruibili.
Per l'accesso ai dati personali e/o sensibili, si prevede l'utilizzo di un codice identificativo personale, assegnato e gestito in modo tale che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore a sei mesi.
Un medesimo codice identificativo personale non può essere utilizzato per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.
Tutti i dati personali sono residenti su server e quindi soggetti alle procedure giornaliere di salvataggio gestite a livello centralizzato.

Tutti gli ambienti nei quali sono custoditi dati personali e/o sensibili dovranno essere dotati di chiavi di sicurezza non duplicabili.
Per quanto riguarda la sicurezza fisica sono presenti e costantemente controllati dal responsabile della sicurezza fisica impianti di rilevazione fumi e antincendio, e l'area nella quale sono custoditi i sistemi è collocata in zona non a rischio ambientale. La SALA SERVER è dotata di impianto di continuità elettrica e di condizionamento.

Al fine di poter recuperare i dati a seguito di qualsiasi calamità, si prevede di predisporre SEMPRE UNA COPIA DEI DATI con una frequenza giornaliera per le aziende con più di 10 addetti ed almeno settimanale per quelle di dimensioni inferiori. La copia potrà essere eseguita con qualsiasi idoneo mezzo (nastri magnetici, CD, DVD, altri supporti per la memorizzazioni e di massa). Le copie dovranno essere segregate in altri locali rispetto a quelli in cui sono dislocati i supporti di memorizzazione, al fine di preservarle in caso di furto o incendio, dovranno essere custodite a chiave ed affidate al responsabile della custodia dei dati secondo le disposizioni impartite nella lettera d'incarico.

Annualmente sarà necessario dare evidenza oggettiva di aver condotto un test di recupero dati dalla copia per verificare l'efficienza del sistema.

| | |
|---|---|
| **Criteri individuati per il salvataggio (procedure operative in essere)** | SI EFFETTUANO COPIE DI SICUREZZA DEI FILE (DOCUMENTI, APPLICAZIONI, ECC.) SU SERVER DI BACKUP. I DATI PERSONALI, ATTRAVERSO LA PROCEDURA DI BACKUP, VERRANNO ARCHIVIATI CON FREQUENZA GIORNALIERA, GARANTENDONE IN OGNI CASO L'1NTEGRITA' E DISPONIBILITA', L'AGGIORNAMENTO E LA CONSISTENZA CON GLI ALTRI DATI CORRELATI,<br>NONCHE' IL TEMPESTIVO RIPRISTINO IN CASO DI PERDITA |
| **Responsabile del Backup** | 3g Innovation Tecnology Sri; |
| **Istruzioni Per il Backup** | DOPO AVER IMMESSO LA PASSWORD, LA PROCEDURA DI BACK-UP VIENE ESEGUITA IN AUTOMATICO |
| **Periodicità del Backup** | GIORNALIERO |
| **Luogo di Conservazione klelBackup** | SERVER SALA APPARATI |
| **Istruzioni per la Verifica del Backup** | CONTROLLO INTEGRITA' DEI FILE |
| **Pianificazione prove di ripristino** | Nanuale |
| **Responsabile prove ripristino Backup** | 3g Innovation Tecnology Sri VIA D'AMATO, 3/L, 86100, Campobasso |
| **Istruzioni per il Ripristino del Backup** | PRIMA DI EFFETTUARE IL RIPRISTINO DEI DATI VIENE VERIFICATA LA DISPONIBILITA' OPERATIVA DEL SERVER E LA CONGRUITA' DELLE APPLICAZIONI. LE PROVE DI RIPRISTINO VENGONO TESTATE ANNUALMENTE E LE PROCEDURE<br>DI RESTORE SONO ESEGUITE DA PERSONALE QUALIFICATO |
| **Strumento di Backup** | SERVER |

Per il ripristino dei dati il responsabile dei servizi informativi o un suo incaricato dovrà verificare almeno ogni mese il funzionamento di questa attività. Dovrà procedere alla copia di back-up dei dati dal supporto prescelto e attivare la procedura di ripristino verificando che il dato è effettivamente a disposizione.

Al fine di garantire che non si interrompa l'attività produttiva per un black-out che provochi perdite di dati o non reperibilità degli stessi è stato predisposto un adeguato potenziamento dell'impianto elettrico. Gli strumenti informatici sono messi in condizione di essere ripristinati rapidamente.

## PROCEDURA DI GESTIONE DI POSSIBILI VIOLAZIONI DEI DATI (DATA BREACH)

Informare immediatamente, verbalmente e riservatamente il proprio superiore in linea gerarchica e far seguire a stretto giro (entro e non oltre minuti 15) e-mail, sempre a proprio superiore gerarchico, riportante la segnalazione e accurata descrizione della situazione, mettendo in copia, altresì, l'indirizzo: ufficioprivacy@3gspa.net ed al preposto alla verifica della applicazione delle policy in tema privacy, individuato nel Responsabile della Sua Unità Operativa/Ufficio/Area, mettendo come oggetto: possibile DATA BREACH.
L'Ufficio Privacy procede pertanto, raccolte le informazioni utili alla valutazione della gravità e dell'entità del potenziale breach, ad allertare il top management (Amministratore Unico -

Direttore Generale – Direttore di Produzione) e le funzioni che ritiene utili (es. Amministratore di Sistema – Responsabile Ufficio Legale – Data Protection Officer).
La commissione così convocata, ove necessario con l'ausilio di un consulente esterno, decide se attivare o meno il Data Protection Officer per la messa in opera delle eventuali comunicazioni all'Autorità Garante e notifica agli interessati.
Si procede in ogni caso all'annotazione della violazione o della potenziale violazione sul Registro dei Trattamenti, secondo le disposizioni di Legge e a riunione di debreafing da effettuarsi nella settimana successive alla violazione\potenziale violazione per valutare ulteriori misure e valutare la gestione del breach.

**ALLEGATI**

- Format nomina incaricato al trattamento dei dati personali;
- Format nomina preposto alla verifica del corretto adempimento alla policy privacy ed alla normativa vigente;
- Format nomina responsabile esterno del trattamento ex art. 28 GDPR;
- Formati informative dipendenti e collaboratori;
- Format norme gestione password;
- Format informativa dipendenti;
- Format informativa collaboratori;
- Format informativa candidati recruiting;
- Valutazione rischi sicurezza informatica.
- Valutazioni di Impatto effettuate
- Procedura per la verifica della esattezza dei data base
- Procedura per l'inoltro massivo di dati personali (CEDOLINI E CUD)
- Certificato ISO 27001

-