MANUALE GDPR
adottato ai sensi dell'art. 24 del Regolamento UE 2016/679

Sommario

1 - SCOPO DEL MANUALE GDPR

GR Elettronica S.r.l. (di seguito "società"), al fine di dimostrare che il trattamento dei dati personali è effettuato in conformità al Regolamento UE 2016/679 (General Data Protection Regulation - di seguito per brevità "GDPR"), ha predisposto il presente documento denominato "Manuale GDPR".

Questo documento è approvato ed aggiornato dall'alta direzione e dal personale aziendale, con l'ausilio ed il supporto del Responsabile della Protezione dei dati personali (RPD).

Il presente manuale sostituisce il "Documento Programmatico sulla Sicurezza" (per brevità DPS), che la società ha continuato ad aggiornare fino al 2017, e rappresenta lo strumento operativo e gestionale per programmare e verificare l'adozione delle misure tecniche e organizzative adeguate, secondo quanto previsto dagli articoli 24 e 32 del GDPR.

Il Manuale GDPR, pertanto, costituisce un valido strumento per:

- definire compiti, istruzioni e responsabilità dei soggetti, che a vario titolo sono preposti al trattamento dei dati personali e all'adozione delle misure tecniche ed organizzative di sicurezza e di protezione;
- descrivere le politiche aziendali, nonché le azioni e gli adempimenti adottati per garantire un livello di sicurezza adeguato;
- individuare indirizzi e misure per consentire la gestione delle emergenze e garantire la continuità operativa ed il ripristino degli strumenti e dei dati;
- indicare azioni per consentire il controllo del sistema di sicurezza.

Il presente manuale è strutturato in paragrafi e allegati:

- i paragrafi recano la descrizione delle azioni da adottare e delle regole generali da rispettare, per cui sono conoscibili da tutti;
- gli allegati contengono le indicazioni operative e la descrizione delle misure tecniche ed organizzative adottate dalla società (per cui di norma non sono pubblici, in quanto costituiscono documenti aventi natura riservata e riferita a processi critici).

2 – PROFILI SOGGETTIVI - CHI

2.1. Titolare e responsabili del trattamento

La disciplina europea in tema di protezione dei dati personali (GDPR), in continuità rispetto al codice della privacy italiano, individua due figure soggettive particolari, aventi una responsabilità specifica per quanto concerne il trattamento dei dati personali:

a) il **titolare del trattamento**: è la GR Elettronica s.r.l. (di seguito per brevità "società"), come entità considerata nel suo complesso, rappresentata dall'amministratore pro-tempore;
b) il **responsabile del trattamento** (art. 28 GDPR): è la persona fisica o la persona giuridica che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e avvenga nel rispetto dei diritti dell'interessato.

I responsabili del trattamento possono essere individuati sia all'interno dell'organizzazione aziendale (quindi, nella figura di dipendenti della società), sia all'esterno, nelle figure che in base ad un contratto o ad un atto prestano servizi o svolgono un'attività per conto della società e quindi sono preposte ad eseguire operazioni di trattamento in nome e nell'interesse della stessa.

A tal fine, la società predispone ed aggiorna un elenco di tutti i fornitori, consulenti e collaboratori esterni, ai quali sono affidati attività e compiti che comportano la necessità di accedere agli strumenti elettronici aziendali e quindi ai dati personali, per cui occorre formalizzare la designazione in qualità di responsabile del trattamento.

L'elenco dei soggetti da designare in qualità di responsabili è riportato in allegato **AL01**.

Ai soggetti esterni possono essere affidati sia compiti di natura operativa (concernenti le operazioni di trattamento), sia funzioni di gestione degli strumenti con profili di accesso privilegiati, per cui sono assegnate funzioni di amministrazione di sistema.

A ciascun soggetto, indicato nell'allegato AL01, è quindi conferita la qualità di responsabile del trattamento, utilizzando, a seconda che si tratti di un dipendente della società o di un soggetto esterno, la apposita lettera di nomina (**AL02.01 e AL02.02**), predisposta ai sensi dell'art. 28 del RGDP.

Quindi, ai responsabili sono affidati i compiti e le funzioni ivi indicate, comprese, ove necessario, anche quelle relative all'amministrazione dei sistemi.

2.2. Autorizzati al trattamento dei dati personali (*alias* incaricati del trattamento)

Il titolare o il responsabile del trattamento svolge le operazioni di trattamento mediante la preposizione e l'ausilio di persone fisiche: si tratta dei soggetti autorizzati al trattamento (ai sensi dell'art. 29 GDPR), che, in continuità rispetto al codice della privacy, possono continuare ad essere chiamati incaricati del trattamento.

Secondo la definizione riportata nel GDPR si tratta di "chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento, dovendo essere istruito con un atto scritto".

Gli autorizzati al trattamento possono essere sia soggetti interni all'organizzazione aziendale, sia soggetti esterni, che operano autonomamente oppure all'interno di una organizzazione.

La designazione degli autorizzati al trattamento (*alias* incaricati del trattamento) è effettuata dal responsabile del trattamento ed avviene mediante una apposita lettera, il cui formato generale è riportato in allegato (**AL03**).

2.3. Responsabile della Protezione dei Dati Personali (RPD)

Ai soggetti indicati nei due paragrafi precedenti, con l'adozione del GDPR si è aggiunto il Responsabile della protezione dei dati (RPD), che è figura obbligatoria quando il trattamento dei dati è effettuato da un'autorità pubblica ovvero nelle ipotesi previste dall'art. 37 del Regolamento UE 2016/679.

La società, ancorché non obbligata, ha scelto di procedere alla nomina di un RPD, al fine di avere una figura, cui affidare compiti di consulenza e di supporto a favore del titolare e dei responsabili e di sorveglianza dell'osservanza del GDPR.

A tal fine, è stato designato un esperto in materia di *data protection,* al quale sono stati affidati i compiti riportati nella lettera di nomina (**AL04**).

3 – ELENCO DEI TRATTAMENTI - COSA

Il Regolamento UE 2016/679 (GDPR) ha ad oggetto la disciplina dell'attività di trattamento dei dati personali.

In particolare:

- per **trattamento** si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, con 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";
- per **dato personale** si intende "**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".

Dall'esame delle definizioni si evince che il GDPR si applica solo ed esclusivamente ai trattamenti di dati personali riferiti a persone fisiche, mentre sono escluse dall'ambito di applicazione del regolamento le informazioni relative alle persone giuridiche.

Sono due le categorie fondamentali di dati personali:

1) **dati particolari:** si intendono i dati che "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona";

2) **dati comuni:** le informazioni riferite a persone fisiche identificate o comunque identificabili, che non siano idonee a rivelare gli stati, i fatti e le qualità, di cui all'art. 9 del GDPR, per i quali è vietato il trattamento, salvo che non ricorrano i presupposti di liceità e di legittimazione, previsti dal comma 2 dell'articolo ivi considerato.

La società, al fine di gestire correttamente le operazioni di trattamento e di dimostrare che il trattamento è effettuato conformemente al Regolamento UE 2016/679, predispone ed aggiorna un elenco degli strumenti elettronici e dei sistemi informatici in uso per il trattamento dei dati personali o comunque considerati critici per i processi aziendali, al fine di avere una mappatura degli strumenti da proteggere.

Inoltre, nel medesimo allegato, unitamente agli strumenti e ai sistemi, è riportato un elenco dei trattamenti di dati personali, costituente la base per l'analisi e la valutazione dei rischi e per il conferimento degli incarichi e la formalizzazione delle autorizzazione e delle istruzioni.
L'elenco degli strumenti e dei sistemi, nonché dei trattamenti dei dati svolti in seno alla società è riportato in allegato (**AL05**).

4 – ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI E PROTEZIONE DEI DAI PERSONALI - COME

4.1. Principi ed obiettivi in materia di sicurezza e determinazione delle modalità di trattamento dei dati personali

Gli obiettivi di sicurezza, che la società si pone con la redazione e l'aggiornamento del presente manuale, sono:

1. dimostrare che sono adottate le misure tecniche ed organizzative adeguate, secondo quanto previsto dall'art. 24 del GDPR;
2. garantire il rispetto del principio della *privacy by design*, ai sensi dell'art. 25, comma 1 del GDPR;
3. mettere in atto le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (*privacy by default*), ai sensi dell'art. 25, comma 2 del GDPR;
4. ridurre, a livelli accettabili e gestibili, i principali rischi di sicurezza, che possono interessare il sistema informativo aziendale;
5. mantenere, compatibilmente con i vincoli di sicurezza previsti dal GDPR e dalle eventuali indicazioni dell'Autorità Nazionale di Controllo, il massimo livello di usabilità del sistema.

La determinazione dei compiti e delle istruzioni da impartire agli incaricati del trattamento è riportata in apposito allegato (**AL06**) e tiene conto altresì dell'organigramma aziendale e dei manuali operativi e di organizzazione, ai quali si rinvia in modo dinamico e funzionale e che costituiscono parte integrante e sostanziale del presente manuale.

4.2. Attività e azioni del titolare del trattamento per la garanzia della conformità dei trattamenti di dati al GDPR

La società, in qualità di titolare del trattamento, provvede a determinare le finalità e le modalità dei trattamenti.

Pertanto, al fine di garantire la conformità delle attività di trattamento dei dati al GDPR, la società procede a:

a) nominare fornitori e soggetti esterni all'organizzazione aziendale (elencati in **AL01**) in qualità di responsabili esterni del trattamento, utilizzando il modello di atto di nomina riportato in allegato (**AL02**);
b) designare in qualità di autorizzati al trattamento (ossia incaricati al trattamento dei dati) le persone fisiche preposte allo svolgimento delle operazioni di trattamento, utilizzando l'apposita lettera (**AL03**);
c) inviare per posta elettronica (all'indirizzo individuale assegnato dall'azienda o a quello dichiarato all'atto della sottoscrizione del contratto di collaborazione) a ciascuna persona (sia dipendente, sia collaboratore strutturato) le istruzioni scritte per il trattamento dei dati (riportate nell'allegato **AL06**);
d) vigilare sul rispetto da parte degli incaricati e dei soggetti nominati in qualità di responsabili esterni delle istruzioni relative alle misure di sicurezza previste dalla società, adottando le misure correttive e integrative necessarie;
e) collaborare, con i soggetti preposti alla gestione e alla amministrazione dei sistemi, alla definizione del profilo di autorizzazione da associare alle credenziali di autenticazione assegnate a ciascun incaricato del trattamento dei dati. Per profilo di autorizzazione si intende "l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti"; il "sistema di autorizzazione" è costituito dall'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
f) provvedere a richiedere la disattivazione, ovvero la variazione del profilo di autorizzazione associato a ciascun incaricato, nel caso in cui la persona fisica cessi di operare all'interno della struttura di propria competenza ovvero, per qualsiasi motivo, fosse stato modificato il suo profilo professionale;

g) vigilare sull'attività svolta dagli incaricati del trattamento, verificando il rispetto delle procedure operative e delle istruzioni impartite dall'azienda, anche in materia di misure di sicurezza.

La società, inoltre, per quanto riguarda la gestione e la manutenzione degli strumenti elettronici, si avvale sia di personale interno, sia di soggetti esterni, che sono nominati amministratori di sistema, in conformità alle indicazioni fornite dal Garante per la protezione dei dati personali nel provvedimento generale del 27 novembre 2008, così come modificato ed integrato con deliberazione del 25 giugno 2009.

La designazione delle persone fisiche in qualità di amministratore di sistema avviene mediante l'utilizzo del modello di lettera di nomina riportata in allegato **AL02**, che deve essere consegnata personalmente ovvero trasmessa a mezzo PEC alla persona o al consulente da nominare in qualità di amministratore di sistema ovvero da designare quale responsabile esterno del trattamento, con funzioni di amministrazione di sistema.

Quest'ultimo è obbligato a sua volta a procedere alla designazione formale delle persone fisiche, preposte allo svolgimento di compiti di amministrazione di sistema, nell'interesse e per conto dell'azienda, che è titolare dei relativi trattamenti di dati.

4.3. – Liceità del trattamento e obblighi di informazione

Il trattamento dei dati personali deve essere svolto in modo lecito, corretto e trasparente, secondo quanto previsto dall'art. 5 del GDPR.

Inoltre, la raccolta dei dati deve avvenire per finalità determinate, esplicite e legittime e i dati possono essere trattati in modo che l'attività da svolgere non sia incompatibile con tali finalità.

Pertanto, all'interessato o alla persona che fornisce i dati, al momento della raccolta degli stessi, deve essere fornita una idonea informativa, nelle forme previste dagli articoli 12 – 13 – 14 del GDPR.

A tal fine, la società ha predisposto un formulario, contenente le diverse informative da utilizzare per tale adempimento.

Oltre, all'obbligo di informativa, affinché il trattamento dei dati sia lecito, occorre che siano rispettate le regole di legittimazione, previste rispettivamente per la raccolta ed il trattamento dei dati comuni e dei dati particolari dagli articoli 6 e 9 del GDPR.

Per quanto concerne i trattamenti di dati personali di cui è titolare la società di norma non occorre l'acquisizione del consenso dell'interessato, considerato che le finalità del trattamento medesimo

sono connesse all'adempimento o al'esecuzione di prestazioni di un contratto di cui è parte l'interessato medesimo ovvero per adempiere un obbligo legale.

La modulistica da utilizzare per adempiere all'obbligo di informativa e all'eventuale raccolta del consenso da parte dell'incaricato (ove necessario) è riportata in allegato **AL07**.

5 –SICUREZZA DEI DATI PERSONALI – PERCHE'

5.1. – Analisi e valutazione dei rischi e piano di sicurezza

L'art. 32 del GDPR prevede che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

La sicurezza può essere definita come "l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite" e dunque "l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco".

I rischi di perdita dei dati, anche accidentale, di accesso abusivo e di trattamento illecito o non consentito dei dati possono essere causati (a titolo meramente esemplificativo) da:

- malfunzionamenti di sistemi hardware e software, applicativi software e servizi;
- persone esterne all'organizzazione (hacker, spie, terroristi, vandali, ecc.);
- eventi naturali (inondazioni, incendi, terremoti, tempeste, ecc.);
- persone interne all'organizzazione;

e possono essere identificati come:

- accidentali,
- deliberati.

Rendere sicuro un sistema informatico non significa esclusivamente attivare un insieme di contromisure specifiche, di carattere tecnologico ed organizzativo, che neutralizzino tutti gli attacchi ipotizzabili al sistema di servizi, ma comporta l'esigenza di collocare ciascuna delle contromisure individuate in una politica organica di sicurezza, che tenga conto dei vincoli (tecnici, logistici, organizzativi, amministrativi e legislativi) imposti dalla struttura tecnica ed organizzativa, in cui la società opera e che giustifichi ciascuna contromisura in un quadro complessivo.

Principale obiettivo di un sistema di sicurezza è quindi la salvaguardia delle informazioni.

A tal fine, per ciascun sistema informativo automatizzato aziendale, per gli strumenti elettronici e per gli archivi e documenti cartacei deve essere fornita la cosiddetta **garanzia "R.I.D."**, ossia "**Riservatezza – Integrità – Disponibilità"**.

Di seguito, per completezza, si riportano le definizioni di ciascuna garanzia:

- **Riservatezza (o Confidenzialità):** solo gli utenti autorizzati possono accedere alle informazioni necessarie;
- **Integrità:** protezione contro alterazioni o danneggiamenti; tutela dell'accuratezza e completezza dei dati;
- **Disponibilità:** le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

Fra le risorse (*asset*) da tutelare rientrano certamente:

- dati digitali;
- documenti cartacei;
- flussi informativi;

nonché componenti materiali come:

- server;
- computer;
- reti;

ma anche:

- il personale;
- gli edifici;
- gli uffici.

L'approccio alla sicurezza deve avvenire in una logica di prevenzione (ossia mediante l'utilizzo di metodologie e di strumenti di *risk management*) piuttosto che in una logica di gestione delle emergenze o di semplice controllo / vigilanza.

L'architettura del sistema, al fine di garantire le esigenze di sicurezza di protezione degli strumenti e dei dati, si basa su 3 elementi fondamentali:

- le politiche aziendali di sicurezza;
- le soluzioni organizzative e tecnologiche;

- gli atteggiamenti individuali.

Un sistema di gestione della sicurezza delle informazioni efficiente ed efficace permette all'organizzazione di:

- mantenersi aggiornata su nuove minacce e vulnerabilità e prendere le medesime in considerazione in modo sistematico;
- trattare incidenti e perdite in ottica di prevenzione e di miglioramento continuo del sistema;
- sapere in tempo utile quando politiche di sicurezza e procedure non sono implementate, per prevenire potenziali danni;
- implementare politiche e procedure di primaria importanza.

Le misure tecniche ed organizzative devono essere adottate mediante l'utilizzo di un **processo di autodeterminazione**, per cui occorre provvedere alla riduzione dei rischi, che possono interessare i dati personali oggetto di trattamento in seno all'azienda e che riguardano il sistema informativo nel suo complesso.

Il sistema di protezione dei dati personali della società si basa sui seguenti principi generali:

- tutte le informazioni (dati, documenti, archivi, …) devono essere protette e disponibili;
- al fine di garantire la riservatezza dei contenuti e delle informazioni, la sicurezza deve riguardare anche le reti di comunicazioni elettroniche dei dati;
- si deve procedere alla previsione di misure di sicurezza per la protezione di aree e locali, in cui sono localizzati i server, considerati "sensibili" per l'attività dell'azienda, e gli archivi cartacei, monitorandone le caratteristiche tecniche e le misure di tutela dagli accessi non autorizzati;
- tutte le operazioni di trattamento dei dati, effettuate utilizzando strumenti connessi alla rete di comunicazione elettronica, devono essere oggetto di tracciabilità, garantendo il non ripudio delle operazioni svolte, dovendo utilizzare un sistema di autenticazione informatica, che consenta un controllo dell'identità di "chi sta facendo che cosa";
- devono essere predisposte misure tecniche ed organizzative di sicurezza per l'accesso ai locali, che ospitano i server e gli strumenti elettronici in dotazione, favorendo possibilmente la localizzazione e l'ubicazione in unico luogo o in luoghi collegati, al fine di consentire una migliore gestione degli strumenti e della sicurezza attiva e passiva;

- ogni eventuale incidente o evento straordinario, che possa pregiudicare la sicurezza dei dati e dei sistemi, deve essere oggetto di analisi e di rapporto scritto;
- tutti i progetti per lo sviluppo di nuovi sistemi / servizi, aventi natura trasversale e che possano interessare il sistema informativo dell'azienda, devono essere comunque gestiti secondo quanto riportato nel presente manuale;
- al pari, tutte le modifiche eventualmente apportate ai processi organizzativi devono essere documentate nel presente manuale o nei documenti del sistema di qualità aziendale.

In particolare, l'analisi e la valutazione dei rischi sono effettuate utilizzando la tabella riportata in allegato (**AL08**), mediante l'individuazione delle singole minacce e vulnerabilità, per le quali si è provveduto a determinare il peso del rischio in termini di probabilità (P) e di danno (D), valutati secondo i parametri (alto – medio – lieve) associati a ciascuna minaccia.

All'esito dell'analisi e della valutazione dei rischi, si procede alla determinazione delle misure tecniche ed organizzative di sicurezza, ai sensi dell'art. 32 del GDPR, elencate e descritte nel Piano di sicurezza riportato in allegato **AL09**.

Il piano di sicurezza è strutturato in tre parti:

1) descrizione delle misure di sicurezza adottate all'esito dell'attività di analisi e valutazione dei rischi, secondo quanto riportato in allegato AL08;
2) piano delle emergenze: riguarda gli eventi naturali (ossia i disastri) ovvero le azioni umane colpose o deliberate che possono determinare una interruzione dei processi lavorativi o della continuità dei flussi informativi, con blocchi e non conformità. Il piano delle emergenze è 5.2. Gestione dell'emergenza e ripristino della disponibilità dei dati e degli strumenti adottato al

fine di garantire la conformità alle norme in tema di certificazione, per cui si rinvia alla documentazione aziendale in uso;

3) manuale operativo: è uno strumento in cui sono descritte le misure tecniche ed organizzative di sicurezza e i suggerimenti per procedere in modo corretto all'uso dei dispositivi e allo svolgimento delle operazioni di trattamento.

La società, nell'ambito del sistema di certificazione dei processi aziendali, ha predisposto un piano di analisi e di valutazione di attività e accadimenti che possono determinare interruzioni o blocchi dei processi produttivi (piano richiamato nell'allegato **AL09**, cui si rinvia).

Si tratta di accadimenti che incidono sui processi aziendali e produttivi, che costituiscono il *core business* aziendale, per i quali occorre adottare un'attenta analisi e valutazione.

Sotto il profilo della *data protection*, con l'espressione "continuità operativa" si intende "l'insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso".

Al fine di garantire la continuità operativa dei sistemi e quindi dei trattamenti di dati personali, nonché allo scopo di fronteggiare eventi che possano causare il danneggiamento degli strumenti elettronici e la distruzione o perdita delle informazioni cd. critiche, si devono prevedere azioni per fronteggiare l'emergenza e le possibili interruzioni dei processi produttivi.

Le soluzioni di continuità prendono in considerazione, quindi, l'effetto di un evento e non le sue cause.

Al contrario, la prevenzione degli eventi è generalmente demandata a forme di intervento (quali ad esempio l'adozione di misure per la sicurezza e l'integrità fisica degli strumenti e dei dati) non classificabili come "soluzioni di continuità".

Al fine di garantire la continuità dell'attività produttiva, la società, nell'ambito del piano dell'emergenza (indicato o comunque richiamato nell'allegato **AL09**), definisce:

a) le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. La società verifica la funzionalità del proprio piano di continuità operativa con cadenza annuale;

b) il **piano di *disaster recovery*** (costituente parte integrante di quello di continuità operativa, richiamato alla lettera a): questo stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

Il piano di continuità operativa della società ha ad oggetto le attività ed i processi di natura critica.

La redazione del piano e l'adozione delle misure di garanzia della continuità operativa avvengono nel rispetto dei seguenti principi:

1) analisi del contesto e delle possibili emergenze, conseguenti ad eventi naturali o accadimenti / condotte umane, che causino la distruzione o perdita di dati e strumenti ovvero il blocco del sistema con conseguente arresto dell'attività istituzionale e di servizio;
2) identificazione degli eventi che possono comportare una interruzione della continuità operativa da prendere in considerazione;
3) individuazione degli eventi pianificati e degli eventi "non pianificati" che possono determinare una interruzione della continuità operativa;
4) individuazione, per ogni servizio o processo cd. critico da proteggere, dell'insieme delle risorse (umane, tecnologiche, procedurali e gli spazi di lavoro) necessarie a ripristinare l'erogazione;
5) determinazione delle misure necessarie per mantenerne l'operatività. Conseguentemente, occorre prevedere procedure per garantire la continuità operativa (in particolare copia e recupero dei dati, sistemi paralleli);
6) programmazione delle misure per il ripristino dei dati personali a seguito di eventi di distruzione o danneggiamento;
7) individuazione delle misure di sicurezza da adottare per la garanzia della continuità operativa e per il ripristino dei dati e dei sistemi entro un termine massimo di sette giorni dall'evento;
8) programmazione della verifica, da parte della funzione interna di controllo, del corretto funzionamento dei sistemi e delle procedure organizzative per la continuità operativa e il ripristino dei dati, sia da parte di personale interno, sia di soggetti esterni incaricati dell'adozione delle procedure e della realizzazione dei sistemi.

Per definire in che misura un sistema critico deve essere mantenuto in operatività si considerano due indicatori:

1) **RTO** ("**Recovery Time Objective**" - massimo tempo di indisponibilità del servizio), cioè il tempo entro il quale il servizio deve essere ripristinato;

2) **RPO** ("**Recovery Point Objective**", perdita dati sostenibile), in termini di distanza temporale tra il verificarsi dell'emergenza e l'ultimo salvataggio utile e ripristinabile dei dati.

A titolo esemplificativo, la necessità che un servizio o un processo sia riattivato entro 48 ore da un'emergenza e che non si perdano più di 6 ore di operazioni di aggiornamento dei dati, richiede di fissare i seguenti parametri:

- RTO = 48 h;
- RPO = 6 h.

Lo studio del contesto è caratterizzato da due fasi:

1) analisi dei rischi: si determinano i rischi a cui è soggetta un'unità di trattamento cd. critica o un servizio erogato; si analizzano le vulnerabilità; si identificano le possibili salvaguardie;

2) *business impact analysis*: ha lo scopo di determinare le conseguenze derivanti dal verificarsi di ciascun evento critico e di valutarne l'impatto sull'operatività dell'organizzazione.

Il piano delle emergenze e della continuità operativa e di gestione del ripristino dei dati (riportato nella sezione 2 dell'allegato – **AL09**) prende in considerazione almeno i seguenti scenari di crisi:

- distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche per ciascuna unità di trattamento;
- indisponibilità di personale essenziale per il funzionamento o la garanzia della continuità degli strumenti cd. critici;
- interruzione del funzionamento delle infrastrutture (tra cui alimentazione elettrica, reti di comunicazione elettronica, blocco o danneggiamento degli strumenti);
- alterazione dei dati a seguito di attacchi dolosi;
- indisponibilità dei sistemi e degli strumenti a seguito di attacchi dolosi di terzi.

Il piano di continuità e di ripristino indica:

- le misure necessarie per ridurre l'impatto di un'emergenza;
- le risorse alternative a quelle non disponibili;
- le misure organizzative per governare il sistema durante l'emergenza;
- le procedure per gestire il rientro alla normalità.

Nel predisporre il piano di ripristino (cd. piano di *disaster recovery*), si deve provvedere nel seguente modo:

1) definizione di ruoli e di responsabilità;
2) analisi degli eventi che possono causare la distruzione o il danneggiamento dei dati o degli strumenti elettronici;
3) descrizione delle azioni da intraprendere in caso di emergenza al fine del ripristino dei dati e del sistema.

Al fine di garantire la continuità operativa e di verificare l'operato degli amministratori di sistema e la conformità delle misure di sicurezza alla disciplina rilevante in tema di *data protection*, la società nomina un soggetto, in posizione di indipendenza e terzietà, utilizzando il modulo in allegato – **AL10,** al quale affidare funzioni di controllo e di vigilanza, anche al fine di garantire la conformità delle misure di sicurezza e di protezione al GDPR, ai sensi degli articoli 24 e 32 del Regolamento UE 2016/679.

Elenco allegati Manuale GDPR

Documento	Descrizione	Ultima Revisione	Causali aggiornamento	Destinatari	Modalità distribuzione
AL01	Elenco fornitori, consulenti e collaboratori esterni	25/05/2018	Prima redazione	Documento riservato	Documento interno
AL02.01	Lettera designazione responsabile interno del trattamento	31/01/2019	Prima revisione	Dipendenti società	Designazione tramite consegna cartacea o pubblicazione in area riservata sito o invio per posta elettronica
AL02.02	Lettera designazione responsabile esterno del trattamento	31/01/2019	Prima revisione	Fornitori, consulenti e collaboratori società	Designazione tramite invio della lettera per PEC all'indirizzo indicato nel portale www.inipec.gov.it
AL03	Lettera designazione autorizzati al trattamento	31/01/2019	Prima revisione	Dipendenti, collaboratori, lavoratori interinali, consulenti	Designazione tramite consegna cartacea o pubblicazione in area riservata sito o invio per posta elettronica
AL04	Designazione responsabile della protezione dei dati personali	25/05/2018	Prima redazione	Responsabile Protezione Dati (RPD)	Invio tramite PEC al soggetto individuato
AL05	Elenco degli strumenti elettronici e dei trattamenti dei dati personali	25/05/2018	Prima redazione	Documento riservato	Documento interno
AL06	Istruzioni in tema di trattamento dei dati	31/01/2019	Prima revisione	Responsabili del trattamento Autorizzati al trattamento	Consegna mediante invio per PEC ovvero pubblicazione in area riservata o consegna manuale
AL07.01	Formulario informative e modulistica per consenso	31/01/2019	Prima revisione	Clienti, Fornitori, Dipendenti, collaboratori, lavoratori	Inserire informativa su bolle, fatture, mail Consegna a ciascun dipendente o collaboratore all'atto dell'assunzione o della sottoscrizione del contratto Raccolta del consenso, ove necessario, mediante sottoscrizione di una copia del modulo
AL07.02		25/5/2018	Prima redazione		
AL07.03		25/5/2018	Prima redazione		
AL08	Analisi e valutazione dei rischi	25/05/2018	Prima redazione	Documento riservato	Documento interno
AL09	Piano di sicurezza	31/01/2019	Prima revisione	Documento riservato	Documento interno

Documento	Descrizione	Ultima Revisione	Causali aggiornamento	Destinatari	Modalità distribuzione
AL10	Nomina addetto alla funzione di controllo e vigilanza	25/05/2018	Prima redazione	Addetto alla funzione di controllo e vigilanza	Sottoscrizione per presa visione e ricevuta di una copia della lettera di incarico al conferimento incarico