

DOCUMENTAZIONE DI SISTEMA PRIVACY E PROTEZIONE DATI PERSONALI

EDIZIONE n. (Anno 2018-19)

Istruzione operativa : **ADADS- bak679**
Versione : Rif. : VAAS679, DISI679, RMOADS679, **ADADS- SWE679**
Ultima revisione : MIGRAZIONE INCARICHI GDPR-EU/REG.2016/679

Atto di nomina
"AMMINISTRATORE DI SISTEMA BACKUP CONTROLLER"
mansionato per la Gestione di Sistemi di BackUP - ADS-BAK

Tra

Titolare Designante :
Sede Legale Titolare :
Codice Fiscale / Partita IVA :
Legale Rappresentante :

ADS-BAK Designato :
Sede ADS-BAK :
Codice Fiscale / Partita IVA :
Legale Rappresentante :

Il Titolare in qualità di Titolare del Trattamento ("TDT" o "Designante") dei dati personali ai sensi del Regolamento EU 2016/679, nonché controparte nel contratto di servizi stipulato con terzi, e l'ADS-BAK sono di seguito definiti congiuntamente "Parti" e in singolo come "Parte".

Le parti firmano il cartiglio del presente atto sia in frontespizio e che in calce al documento e considerando l'allegato A - "Istruzioni su diligenze dovute per le misure tecnico-organizzative del trattamento dei dati" in presa visione e accettazione dal Designato quale parte integrante del presente Atto a titolo di Privacy Level Agreement (PLA) e Accordi Vincolanti di Impresa (AVI)

Luogo:

Data:

Titolare del Trattamento

Timbro e firma ADS-BAK

Legale Rappresentante

.....

.....

SPPD

Framework

M.S.P.

Premessa:

• che la Designante richiede un contratto di servizio avente ad oggetto le attività connesse all'assistenza informatica specialistica per lo sviluppo, la gestione e la Gestione dei Sistemi di Backup (di seguito **Backup Controller**), che si articola nelle seguenti attività:

- o *installazione, configurazione e collaudo del software per le Copie di Sicurezza dei dati*
- o *controllo del regolare funzionamento del software per le Copie di Sicurezza dei dati*
- o *coordinamento delle attività correttive, manutentive, diagnostiche e di miglioramento delle performance di funzionamento del software per le Copie di Sicurezza dei dati;*
- o *erogazione di attività di formazione in ambiente d'esercizio del software per le Copie di Sicurezza dei dati*

• che per tali attività il Titolare ricoprirà le funzioni di Responsabile esterno al trattamento dei dati informatici affidati (**Art. 28 del Regolamento EU 2016/679**);

• che per tali attività il Titolare potrà designare anche una figura che ricoprirà le funzioni di Amministratore di Data Base (**DBA**);

considerato:

• che per preparazione ed esperienza lei fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nella gestione e nel trattamento dei dati;

• il provvedimento generale del Garante per la protezione dei dati personali "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" del 27 novembre 2008 e successive modifiche ed integrazioni;

• quanto stabilito dall'**Art. 5 del GDPR**, che individua nel Titolare il soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina in tema di trattamento dei dati personali; e nell'**Art. 24**, in cui è indicato che il Titolare del trattamento il debba mettere in atto (nonché riesaminare ed aggiornare) adeguate misure tecniche ed organizzative, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità ai principi fondamentali della disciplina in materia;

con il presente Atto di designazione

avendo valutata l'esperienza, la capacità e l'affidabilità del designato, tenuto anche conto del curriculum e del suo contenuto (*inclusi, attività svolte, titoli di studio, certificazioni professionali, esperienze professionali, corsi di formazione, ecc.*), considerata inoltre la natura delle attività attualmente svolte, relativamente a quanto di seguito indicato,

le conferisce

SPPD

Framework

M.S.P.

il compito di sovrintendere all'installazione, allo sviluppo, alla gestione ed al controllo SW, in qualità di **Backup Controller ADS-BAK**, disponendo un nucleo di misure che rispondano a criteri di sicurezza predefiniti e che puntino a bilanciare in maniera adeguata il rischio a contrasto del quale vengono chiamate, in conformità con quanto definito nell'intesa sottoscritta per i trattamenti interni alla organizzazione del Titolare o eventuali commesse e contratti di servizio con clienti terzi.

Per meglio identificare le attività che le vengono richieste, le indichiamo una serie di servizi a cui dovrà richiamare il compito affidatole:

- **System ACL Security** - impostare un sistema di autenticazione informatica e di gestione delle credenziali di autenticazione, per l'accesso agli elaboratori;
- **Data ACL Security** - adottare un sistema di autorizzazione, costituito dall'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati ed alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione attribuito agli incaricati;
- **Data Crypto Security** - impostare un sistema che consenta la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- **System Configs Disaster recovery/Business continuity** - impostare un sistema che abbia la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- **Data Integrity Audits** - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- **LOGs ACL registry** - adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; avente le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
- **Data Recovery & Physical Media** - assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery), anche automatici nonché approntare, in accordo con l'amministratore di rete, adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS);
- **Training & Teaching Authorized Subjects** - impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedano le modalità di utilizzo dei sistemi di salvataggio dei dati con frequenza almeno settimanale;

- **Data & Systems Backups** - adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- **Data Integrity Audits** - predisporre un sistema automatico di back-up degli apparati presenti che preveda altresì la storicizzazione dei back-up effettuati.
- **Data Recovery & Physical Media** - organizzare la gestione dei supporti di memorizzazione, la manutenzione hardware, la verifica di eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi quali l'accesso abusivo al sistema informatico o telematico (articolo 615 ter C.C.), la frode informatica (articolo 640 ter C.C.), danneggiamento di informazioni, dati e programmi informatici (articoli 635 bis e ter C.C.), danneggiamento di sistemi informatici e telematici (articoli 635 quater e quinquies C.C.);
- **Data Media Secure Erasure** - indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati (*wiping*) per il loro reimpiego, in conformità al Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici;
- **Data & Systems Audits** - predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, dell'efficacia delle misure di sicurezza adottate, per i trattamenti effettuati con l'impiego di strumenti elettronici;
- **Data Restore Audits** - verificare che il sistema di backup adottato sia perfettamente funzionante e che relative Policy adottate siano attuate nella loro integrità;
- **Data mis-uses** - identificare e segnalare al Titolare casistiche d'utilizzo non conformi alla normativa vigente.

Inoltre, nella sua prestazione dovrà:

- *garantire che le risorse vengano utilizzate dagli utenti della struttura che ne abbiano effettivamente diritto, utilizzando gli opportuni meccanismi di identificazione e autenticazione precedentemente indicati;*
- *coadiuvare il titolare o il responsabile, se nominato, della struttura presso la quale presta la sua opera, nella definizione della politica di sicurezza e del regolamento interno di gestione delle risorse informatiche;*
- *consigliare la struttura nella scelta delle dotazioni informatiche, partecipando al processo decisionale teso ad individuare le scelte più vantaggiose;*
- *svolgere un ruolo di prima interfaccia nel caso di incidenti di qualsiasi genere che riguardino i sistemi cui è assegnato e preoccuparsi di erogare una corretta informazione verso gli utenti interni ed esterni; dovrà inoltre supportare il processo di indagine e diagnosi dei problemi ed essere in grado di produrre le necessarie informazioni a tal riguardo*

Sarà infine suo compito riferire periodicamente, ed in ogni caso con cadenza annuale, al Titolare, o al Responsabile del Trattamento (RDT) designato, circa i dati dell'organizzazione nei termini di responsabilità a lei assegnati, circa lo svolgimento dei suoi compiti, dando loro piena collaborazione nello svolgimento delle verifiche periodiche del rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.

La preghiamo di restituirci la presente, firmata per accettazione in ogni sua pagina.

Luogo:

Data:

Titolare del Trattamento

Timbro e firma ADS-BAK

Legale Rappresentante

.....

.....

CLUSOLA SULLA RISERVATEZZA PER TRATTAMENTO DATI TERZI

Ai fini dello svolgimento della sua attività, per conto della nostra organizzazione, potrebbe dover trattare dati di soggetti terzi, qualificati dalla legge in oggetto come **"personali"**, nei limiti necessari per il corretto svolgimento del suo incarico.

Ricordiamo che è fatto divieto di divulgare e comunicare in qualunque modo o forma le informazioni, i dati e le conoscenze riservati ai soggetti terzi che sarà tenuto a trattare; tali informazioni, dovranno essere utilizzate nella misura e con mezzi adeguati e strettamente necessari allo svolgimento delle attività a lei incaricate, previste dal contratto di lavoro corrente o dagli accordi vigenti e con modalità che non compromettano in alcun modo il carattere della riservatezza o arrechino altrimenti danno. Le informazioni, i dati e le conoscenze riservati non potranno essere copiati o riprodotti in tutto o in parte sia con strumenti cartacei che elettronici, se non per esigenze operative strettamente connesse allo svolgimento delle attività commissionate.

Dove necessario, riceverà caso per caso e di volta in volta, istruzioni dettagliate su come debbano essere trattati determinati dati, al fine di ottemperare a quanto previsto dalla normativa di riferimento.

In caso di sua inadempienza, la considereremo responsabile nei nostri confronti, limitatamente alle operazioni effettuate senza la diligenza dovuta in esecuzione delle istruzioni ricevute, ferme in ogni caso le sue responsabilità civili e penali in caso di abuso dei dati personali, di cui sia venuto a conoscenza in esecuzione del rapporto instaurato con noi.

firmata per presa visione ed accettazione.

ADS-BAK designato

.....

SPPD

Framework

M.S.P.