L'OFFICINA DELL'AIAS Coop. Soc.
Via San Michele, 1 - 37141 Verona (VR)
P.IVA: 02924130236

Documento Riepilogativo del Sistema Privacy

Redatto in base alle disposizioni del
GDPR 2016/679
e della normativa nazionale vigente in materia di trattamento e protezione dei dati personali

STAMPATO IL 09/10/2020

In data 09/10/2020 si provvede a redigere il presente Documento Riepilogativo del Sistema Privacy secondo quanto stabilito dalla normativa a tutela della protezione dei dati (GDPR 2016/679 e normativa nazionale vigente). Il documento è composto di 73 facciate.

L'OFFICINA DELL'AIAS Coop. Soc.
Cerpelloni Claudio

Indice

8

1 Documento Riepilogativo del Sistema Privacy

Redatto in base alle disposizioni del
GDPR 2016/679 e della
Normativa nazionale vigente in materia
di trattamento e protezione dei dati personali
E
DEI PROVVEDIMENTI DELL'AUTORITA' GARANTE

1.1 Revisione

Indice delle revisioni

EDIZIONI DEL Documento Riepilogativo del Sistema Privacy (DRSP)					
Nr	**DATA**	**Descrizione delle modifiche**	**Redatto**	**Verificato**	**Approvato**
01	07.02.2017	Edizione in conformità ai requisiti del GDPR 2016/679 e della normativa nazionale vigente	Cerpelloni Claudio L'OFFICINA DELL'AIAS Coop. Soc. ISO Engineering	Cerpelloni Claudio L'OFFICINA DELL'AIAS Coop. Soc.	Cerpelloni Claudio L'OFFICINA DELL'AIAS Coop. Soc.
02	09.10.2020	Edizione in conformità ai requisiti del GDPR 2016/679 e della normativa nazionale vigente	Cerpelloni Claudio L'OFFICINA DELL'AIAS Coop. Soc. ISO Engineering	Cerpelloni Claudio L'OFFICINA DELL'AIAS Coop. Soc.	Cerpelloni Claudio L'OFFICINA DELL'AIAS Coop. Soc.

Revisione delle SEZIONI del Documento Riepilogativo del Sistema Privacy							
Sez.	**TITOLO SEZIONI**	**REVISIONI**					
		00	**01**	**02**	**03**	**04**	**05**
01	Introduzione	02.07.17	28.12.18				
02	Le figure Privacy	02.07.17	28.12.18				
03	Trattamenti con Strumenti Elettronici	02.07.17	28.12.18				
04	Trattamenti senza l'ausilio di Strumenti Elettronici	02.07.17	28.12.18				
05	Diritti dell'interessato	02.07.17	28.12.18				
06	Amministratori di Sistema	02.07.17	28.12.18				
07	Regolamenti, Disciplinari e Formazione	02.07.17	28.12.18				
08	Allegati	02.07.17	28.12.18				
09	Appendici	02.07.17	28.12.18				

1.2 La finalità del Documento Riepilogativo del Sistema Privacy

Il presente Documento Riepilogativo del Sistema Privacy concerne la progettazione, la valutazione, l'implementazione, il controllo e l'aggiornamento delle misure di sicurezza poste a protezione dei dati personali.

L'esecuzione di tali attività consente, da un lato, la "messa in sicurezza" dei dati personali trattati e, dall'altro, l'avvio di un processo di gestione del sistema stesso caratterizzato dalle verifiche periodiche atte a mantenere nel tempo i livelli di sicurezza raggiunti.

Il Documento è redatto alla luce dei principi espressi dalla normativa a tutela della protezione dei dati (GDPR 2016/679 e normativa nazionale vigente in materia)

L'art. 32 del GDPR 2016/679 ha previsto l'adozione di "idonee e preventive misure di sicurezza", le quali devono essere implementate in caso di trattamento di dati personali.

Infatti, la mancata adozione delle misure idonee fa sorgere in capo a "chiunque essendovi tenuto" delle responsabilità penali ed amministrative e un obbligo risarcitorio ex art. 2050 C.C. e artt. 24 e 82 GDPR 2016/679.

Pertanto questo documento è redatto per soddisfare tutte le misure di sicurezza che debbono essere adottate e valutarne l'idoneità sulla base di un'attenta analisi del rischio.

1.3 La funzione del Documento Riepilogativo del Sistema Privacy

Il Documento Riepilogativo del Sistema Privacy definisce il livello di sicurezza in merito al trattamento dei dati personali.

Il Documento traccia il profilo delle vulnerabilità più diffuse mirando a soddisfare tutte le misure di sicurezza organizzative, fisiche e logiche previste dalla normativa a tutela della protezione dei dati (GDPR 2016/679 e della normativa nazionale vigente in materia).

In sintesi, le tre macroaree di sicurezza, che verranno analizzate nel proseguo del Documento e che rappresentano le misure minime di sicurezza apprestate dal Titolare a tutela dei dati si possono raggruppare in misure riguardanti la:

Sicurezza Fisica: la funzione svolta dalla sicurezza fisica è quella di apprestare tutti i mezzi e gli strumenti necessari per proteggere persone, cose e ambienti dai suddetti rischi. Si suddivide in sicurezza di area preordinata ad evitare accessi fisici non autorizzati e sicurezza delle apparecchiature hardware preordinata alla protezione da manomissione o furti dell'hardware e comprende anche la manutenzione degli stessi;
Sicurezza Logica: la funzione svolta dalla sicurezza logica è quella di proteggere i "dati" attraverso misure di sicurezza di carattere tecnologico (c.d. Information and Communication Technology). Rientrano in questa area i c.d. Sistemi di sicurezza preordinati alla protezione di tutte le piattaforme dati presenti in azienda (in primis mediante autenticazione e controllo accessi); meccanismi di sicurezza preordinati alla creazione del *modus operandi* dei sistemi di sicurezza (cifratura, firma digitale, meccanismi per l'autenticazione ecc.)
Sicurezza Organizzativa: la funzione svolta dalla sicurezza organizzativa è quella di prevedere regole e procedure finalizzate a disciplinare gli aspetti organizzativi del processo di sicurezza fisica e logica. In questa area rientrano tutte le prescrizioni riguardanti la definizione dei ruoli, la distribuzione dei compiti e delle responsabilità. Quindi a titolo esemplificativo rientrano in questa area tutte le procedure relative alla gestione delle contromisure di sicurezza logica; oppure le procedure di gestione per la sicurezza della rete, le procedure riguardanti il personale, le procedure di aggiornamento dei software, le procedure di backup, le procedure di formazione degli incaricati e dei responsabili etc…

Il Documento Riepilogativo del Sistema Privacy riguarda di tutti i dati personali (sensibili, biometrici, genetici, giudiziari e identificativi) trattati per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

La normativa nazionale precedente l'entrata in vigore del GDPR 2016/679 prevedeva la seguente definizione di "Dato Personale" e conseguente classificazione di dati (art. 4 D.Lgs 196/03):

Dato personale: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. I dati personali si classificano in:

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato;
Dati sensibili: 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, nonch. i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualit. di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
Dati anonimi: i dati che ragionevolmente non siano riconducibili direttamente e/o indirettamente ad una persona fisica.

Il GDPR 2016/679 all'art. 4 prevede la seguente definizione di Dato Personale e la sua conseguente classificazione:

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. I dati personali si classificano in:

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
Dati biometrici: i 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.

All'artt. 9 e 10 classifica alcuni dati di "tipo particolare":

Categorie particolari di tipi di dati: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici e dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Viste le definizioni pregresse non in sostanziale contrasto con quanto prevede la normativa europea si ritiene, ai fini del presente documento e del Sistema di Gestione Privacy realizzato in L'OFFICINA DELL'AIAS Coop. Soc. d'adottare le seguenti convenzioni relative alla classificazione dei dati personali:

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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. I Dati Personali sono classificabili in:

Dati Identificativi o Comuni: es. anagrafici (nome, cognome, data di nascita, cittadinanza, stato civile, indirizzo, qualifica professione); documenti di identità (CdI, patente, passaporto); codici di identificazione fiscale (CF, partita IVA persone fisiche); dati di contatto (numero di telefono, indirizzo e-mail, indirizzo fisico); codici identificativi lavoratori (matricola, credenziali di accesso ai sistemi informatici); coordinate bancarie (numero CC, codice IBAN); targa veicolo; dati multimediali (vide, audio); dati di navigazione internet (cookie, log, indirizzo IP); dati di geolocalizzazione; dati di profilazione.
Dati Sensibili o Particolari: ad es. dati idonei a rivelare l'appartenenza a partiti, sindacati, organizzazioni a carattere religioso o filosofico; dati genetici; dati biometrici; dati relativi alla salute (es. gravidanza, malattia, appartenenza a categorie protette).
Dati giudiziari: ad es. dati relativi a condanne penali, ai reati e alle connesse misure di sicurezza (es. dati in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti).
Informazioni non considerate dati personali: ad es. informazioni riconducibili a un soggetto non persona fisica; numero di iscrizione al registro delle imprese di una società; indirizzo e-mail, come info@azienda.com; dati resi anonimi o pseudonimizzati.

1.4 Quadro normativo

1. **Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio** *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*
2. **D.Lgs. 30 giugno 2003 n. 196** *"Codice in materia di trattamento dei dati personali"*
3. **Provvedimento dell'Autorità Garante del 27 novembre 2008** *"Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema"*
4. **Provvedimento dell'Autorità Garante del 8 aprile 2010** *"Provvedimento in materia di videosorveglianza"*
5. **Provvedimento dell'Autorità Garante del 8 ottobre 2011 nr. 370** *"Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro"*
6. **Provvedimento dell'Autorità Garante del 12 maggio 2011 nr. 192** "*Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie"*
7. **Legge del 20 maggio 1970 nr. 300** *"Statuto dei Lavoratori"***, così modificata ed integrata dal Decreto Legislativo n. 151 del 14 settembre 2015**
8. **Provvedimento dell'Autorità Garante del 13 luglio 2016 nr. 303** "*Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro"*
9. **Codici Deontologici**
10. **Autorizzazione Generali**

1.4.1 ALLEGATI

Rif. Allegati 9.0 al presente documento.

1.5 Elenco dei modelli

	Codice	Tipo di documento	Descrizione
X	RDT	Lettera di nomina	Delegato Privacy
X	RST	Lettera di nomina	Delegato interno al trattamento dei dati
X	IDT2	Lettera di nomina	Incaricato al trattamento dei dati personali
	IDT2GR	Lettera di nomina	Incaricati al trattamento dei dati personali, per unità organizzativa e/o mansione omogenea
X	GMSE	Lettera di nomina	Incaricato gestione e manutenzione strumenti elettronici
X	CDP	Lettera di nomina	Incaricato della custodia delle copie delle credenziali
X	BKP	Lettera di nomina	Incaricato delle copie di sicurezza
X	RAL_LCC	Lettera di consegna	Controllo degli accessi alle aree ai locali e consegna chiavi
X	DTEC_W_W2	Addendum Privacy	Responsabile esterno al trattamento dei dati ex art. 28 GDPR 2016/679
X	DTEC_A	Modello	Registro dei trattamenti e delle banche dati
X	DTEC_B	Modello	Elenco delle sedi/uffici in cui vengono trattati i dati
X	DTEC_C	Modello	Scheda riepilogativa del Sistema informativo aziendale
X	DTEC_D	Modello	Sistemi di elaborazione per il trattamento dei dati
X	DTEC_E	Modello	Responsabili a cui è affidato il trattamento dei dati in out-sourcing
X	DTEC_F	Modello	Personale autorizzato al trattamento dei dati
X	DTEC_J	Modello	Distribuzione dei compiti e delle responsabilità
X	DTEC_G	Modello	Permessi di accesso ai dati
X	DTEC_H_N	Modello	Piano di formazione del personale autorizzato al trattamento dei dati
X	DTEC_M	Modello	Criteri e procedure per garantire l'integrità dei dati informatici
X	DTEC_O	Prescrizione	Modalità di protezione dei dati e dei locali
X	DTEC_P	Prescrizione	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
X	DTEC_Q	Prescrizione	Modalità di trattamento senza l’ausilio di strumenti elettronici
X	DTEC_S	Modello	Criteri di assegnazione password nei sistemi di elaborazione
X	DTEC_Z-1	Modello	DTEC_Z-1 – Valutazione Rischi – Tabella Descrittiva
X	DTEC_Z-2	Modello	DTEC_Z-2 – Valutazione Rischi – Tabella Operativa

1.6 Definizioni

1.6.1 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.

1.6.2 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.

1.6.3 Dati sensibili o Particolari
Ad es. dati idonei a rivelare l'appartenenza a partiti, sindacati, organizzazioni a carattere religioso o filosofico; dati genetici; dati biometrici; dati relativi alla salute (es. gravidanza, malattia, appartenenza a categorie protette).

1.6.4 Dati giudiziari
Ad es. dati relativi a condanne penali, ai reati e alle connesse misure di sicurezza (es. dati in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti).

1.6.5 Titolare
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.

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

1.6.7 Delegato al trattamento
Le persone delegate per iscritto di compiere le operazioni di trattamento dal Titolare, che operano sotto la loro diretta autorità, che gestiscono uno o più incaricati a livello direzionale e/o organizzativo e che coordinano le attività di trattamento relativamente alla propria area di competenza.

1.6.8 Incaricato
Le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Delegato.

1.6.9 Interessato
La persona fisica, cui si riferiscono i dati personali.

1.6.10 Comunicazione
Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.6.11 Diffusione
Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.6.12 Dato anonimo
Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

1.6.13 Blocco
La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

1.6.14 Banca dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

1.6.15 Comunicazione elettronica
Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

1.6.16 Misure di sicurezza
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 Delegato privacy mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

1.6.17 Strumenti elettronici
Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

1.6.18 Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

1.6.19 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.

1.6.20 Parola chiave
Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

1.6.21 Profilo di autorizzazione
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.

1.6.22 Sistema di autorizzazione
L'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.

1.6.23 Violazione dei dati personali
La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2 Le figure Privacy

L'impostazione, coerente con le previsione del D.Lgs 196/03 (Codice Privacy), fondata sulle figure del Titolare, Responsabile Interno ed Esterno (art. 29) e dell'Incaricato (art. 30), con il GDPR 2016/679 dev'essere mutata.

In base al nuovo assetto organizzativo il "**Titolare del Trattamento**" rimane, nella sostanza, immutato e descritto nel dettaglio al p. 2.1 seguente.

La figura del "**Responsabile**", definito quale persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4 p. 8 GDPR 2016/679), è da intendersi solo quale soggetto esterno e la sua figura è regolata dall'art. 28 GDPR 2016/679. Tale figura è descritta nel dettaglio al p. 2.2 seguente.

La figura del "Responsabile interno", invece, non è più prevista e al suo posto, grazie all'autonomia organizzativa riconosciuta al Titolare, si ritiene opportuno introdurre la nuova figura del "**Delegato al trattamento**" di dati personali, e del "**Delegato privacy**" di cui al p. 2.3 seguente. La nomina dei Delegati è del tutto facoltativa e lasciata alla libera scelta del Titolare.

Per quanto concerne le figure degli "**Incaricati al trattamento**", previste nel precedente "assetto privacy" (ex D.Lgs 196/03), tali figure sono sostituite da quelle delle "Persone autorizzate al trattamento", usando un'espressione tipica e ricorrente all'interno del GDPR 2016/679. Le autorizzazioni sono rilasciate, se del caso, dal Delegato al trattamento e, come più volte ribadito dall'Autorità di Controllo italiana, manterranno l'indicazione d' "Incaricato". Tale figura è descritta nel dettaglio al p. 2.4 seguente.

Nuova figura e fulcro del processo d'attuazione del principio di "responsabilizzazione" o "accountability" di cui al GDPR 2016/679 è il "**Responsabile della protezione dei dati personali**" (RDP), noto anche come "Data Protection Officer" (DPO), previsto e disciplinato agli articoli da 37 a 39 del GDPR 2016/679, che *dev'essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali* (cit. art. 38 GDPR 2016/679). Tale figura è descritta nel dettaglio al p. 2.5 seguente.

Fig. 1

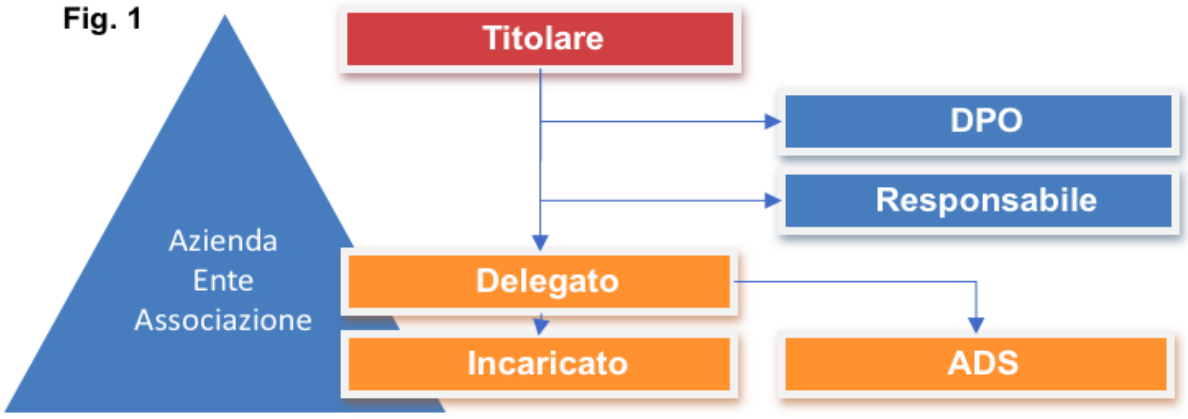

Fig.1: Il nuovo organigramma privacy, previsto dal GDPR 2016/679 ed evoluzione di quello previsto dal già Codice Privacy (D.Lgs 196/03).

2.1 Titolare del trattamento dei dati personali

2.1.1 Nozione di “Titolare del trattamento” dei dati personali

L’art. 4 del GDPR 2016/679 definisce i confini della figura apicale della data protection: il Titolare del Trattamento (vedi Fig. 1)

A norma dell’art. 4 comma 1, lett. f) è "Titolare" del trattamento la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Precisa, l’art.28 che *quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza*.

Il Titolare del trattamento è il soggetto individuato dal legislatore quale centro di imputazione di obblighi e responsabilità.

Il Titolare del trattamento è l’entità nel suo complesso.
L’esercizio della titolarità può essere delegata a persone fisiche dotate di opportuni poteri conferiti con procura.

TITOLARE DEL TRATTAMENTO DEI DATI E’:

L'OFFICINA DELL'AIAS Coop. Soc.
Sede Legale: Via San Michele, 1 - 37141 Verona (VR)
C.F.: 02924130236 P.IVA: 02924130236

Rappresentante Legale: Cerpelloni Claudio

In quanto responsabile giuridico dei trattamenti, il Titolare ha il compito di organizzare e vigilare sul processo di trattamento dei dati personali ed è il destinatario primario delle sanzioni.

Il Titolare del trattamento, ha precisato l’Autorità Garante è il soggetto che decide in modo autonomo *in ordine alle finalità, modalità e* ***sicurezza*** *del trattamento* (Boll. N.2/1997, p.46).
Il Titolare nomina i Responsabili esterni (ex art. 28 GDPR 2016/679) e autorizza al trattamento dei dati tutti i soggetti interni (Delegati e Incaricati) *che procedono al trattamento attenendosi alle istruzioni del Titolare*.

A loro volta il Titolare, i Responsabili o i Delegati interni nominano gli Incaricati al trattamento.

2.2 Responsabile esterno del Trattamento ex art. 28 del GDPR 2016/679

2.2.1 Nozione di Responsabile esterno del trattamento di dati personali

I riferimenti normativi sulla figura del responsabile del trattamento, all'interno del GDPR 2016/679 sono:

art. 4 p. 8) *«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;*
art. 28: *1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*

Il Responsabile del trattamento è il soggetto esterno che tratta dati personali per conto dal Titolare al trattamento dei dati personali.
Richiede l'individuazione e la nomina di un soggetto competente al quale attribuire determinate aree di trattamento da presidiare.

2.2.2 Scelta e Designazione del Responsabile esterno

Il Responsabile va scelto tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni sul trattamento, ivi compreso il profilo della sicurezza.

I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri (c.d. "Addendum Privacy"), che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. L'adesione da parte del responsabile del trattamento a un codice di condotta o a un meccanismo di certificazione approvati, può essere utilizzata come elemento per dimostrare le garanzie sufficienti di affidabilità e sicurezza. Fatto salvo un contratto individuale tra il Titolare del trattamento e il Responsabile del trattamento, il contratto o altro atto giuridico (Addendum Privacy) può basarsi, in tutto o in parte, su clausole contrattuali tipo, anche laddove siano parte di una certificazione concessa al Titolare del trattamento o al Responsabile del trattamento ai sensi degli articoli 42 e 43 del GDPR 2016/679.

L'Addendum Privacy può essere redatto in forma scritta o anche in formato elettronico (Rif. Mod. DTEC_W_W2). Nel caso in cui il Titolare non intenda elargire alcun compenso è opportuno che ciò risulti nell'Addendum Privacy. L'Addendum Privacy va firmato per accettazione. Nell'Addendum Privacy il Titolare deve informare il Responsabile delle responsabilità che gli sono affidate. La designazione del Responsabile è a tempo indeterminato. La cessazione dall'ufficio avviene per revoca e/o dimissione.

In caso di mancata accettazione della designazione da parte del Responsabile, vista la responsabilità diretta del Titolare anche sull'operato di tali soggetti, potrà essere interrotta qualsiasi relazione contrattuale, di fornitura e/o di servizio con il Fornitore stesso. In questo caso ricorre la "giusta causa per inadempimento contrattuale". In ogni caso il Titolare può revocare e/o sostituire il Responsabile a suo insindacabile giudizio in ogni momento e senza preavviso.

L'Addendum Privacy prevede, in particolare, che il Responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32 GDPR 2016/679;

d) rispetti le condizioni previste per ricorrere a un altro responsabile del trattamento. Quando un Responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nell'atto di nomina, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR 2016/679. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.
e) tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR 2016/679;
f) assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR 2016/679, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento;
g) su scelta del Titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato. A tal riguardo, il Responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR 2016/679 o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Il Responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

Il Responsabile, a norma di quanto disposto dall'art. 32 let. d) GDPR 2016/679 dev'essere valutato periodicamente, anche sotto il profilo della sicurezza e dell'affidabilità. Si consiglia che tali valutazioni avvengano almeno annualmente in sede di Audit del Sistema Privacy. La valutazione verrà riportata in un apposito verbale redatto e sottoscritto dal Titolare del trattamento dei dati (DTEC_W_W2_VA).

La medesima procedura di verifica è da applicarsi relativamente ai Responsabili Esterni per il trattamento di dati informatici, come previsto dal Provvedimento del Garante del 27 novembre 2008 recepito in Gazzetta Ufficiale Nr. 300 del 24 dicembre 2008.

Fatti salvi gli articoli 82, 83 e 84 del GDPR 2016/679, se un Responsabile del trattamento viola il GDPR, determinando le finalità e i mezzi del trattamento, è considerato a tutti gli effetti giuridici e legali un Titolare del trattamento in questione.

2.2.3 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti ai soggetti nominati in qualità di "Responsabile del trattamento" esterno:

Codice	Tipo di documento	Descrizione
DTEC_W_W2	Addendum Privacy	Responsabile esterno al trattamento dei dati ex art. 28 GDPR 2016/679
DTEC_W_W2_VA	Verbale	Verbale di valutazione annuale Responsabili ex art. 28

2.3 Delegati al Trattamento

2.3.1 Nozione di Delegati al trattamento

Le persone delegate per iscritto di compiere le operazioni di trattamento dal Titolare, che operano sotto la sua diretta autorità, che gestiscono uno o più incaricati a livello direzionale e/o organizzativo e che coordinano le attività di trattamento relativamente alla propria area di competenza.

Tale figura è designata dal Titolare, anche se per il passato se ne è ravvisata la necessità e l'utilità d'individuazione praticamente in tutte le strutture nelle quali si è proceduto alla realizzazione di un Sistema di Gestione Privacy. Tale figura si può individuare in due particolari soggetti:

Il **Delegato Privacy (RDT)**: è quel soggetto che è chiamato internamente all'organizzazione a gestire il Sistema di Gestione Privacy;
Il **Delegato al Trattamento (RST)**: è quel soggetto che per proprie mansioni gestisce gruppi di persone autorizzate al trattamento.

Il Titolare può ritenere opportuna la nomina di almeno un Delegato Privacy (RDT) a livello aziendale e/o almeno un Delegato al Trattamento (RST) a seconda della propria organizzazione. Inoltre può decidere quale delle due figure individuate può nominare il Personale Incaricato al trattamento dei dati.

Ove necessario per esigenze organizzative, possono essere designati Delegati più soggetti, anche mediante suddivisione di compiti. Tali compiti sono analiticamente specificati per iscritto dal Titolare. Il Delegato effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

2.3.2 Scelta e Nomina dei Delegati al trattamento

Il Delegato è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

L'atto di nomina può essere redatto in forma scritta o anche in formato elettronico (Rif. Mod. LI_RST e LI_RDT). La nomina è riconducibile al contratto di mandato (artt.1703 e seg. c.c.). Il mandato si presume oneroso (art. 1709 c.c.). Nel caso in cui il Titolare non intenda elargire alcun compenso è opportuno che ciò risulti nell'atto di nomina. La nomina va firmata per accettazione. Nell'atto di nomina il Titolare deve informare il Delegato delle responsabilità che gli sono affidate. La nomina del Delegato è a tempo indeterminato. La cessazione dall'ufficio avviene per revoca e/o dimissione.

Il Delegato, su specifica istruzioni del Titolare, può nominare gli Incaricati al trattamento, secondo quanto previsto al successivo paragrafo 2.4.

Al fine di garantire una migliore, lecita ed efficiente gestione delle operazioni di trattamento di dati personali nell'ambito dell'azienda, L'OFFICINA DELL'AIAS Coop. Soc. in qualità di Titolare del trattamento provvede ad individuare un c.d. "**Delegato Privacy**", soggetto al quale sono attribuiti tutti, eventualmente mediante delega deliberata dal C.d.A. medesimo, i poteri necessari a garantire il pieno rispetto da parte di L'OFFICINA DELL'AIAS Coop. Soc. della Normativa secondo la specifica lettera di nomina (Rif. RDT – *"Lettera Nomina Delegato Privacy"*).

DELEGATO PRIVACY (RDT):

Responsabile Privacy (RDT): Cerpelloni Claudio

DELEGATO AL TRATTAMENTO (RST):

Si è deciso di non procedere alla nomina per l'anno in corso per motivi tecnico-organizzativi.

Il Titolare può revocare e/o sostituire il Delegato a suo insindacabile giudizio in ogni momento e senza preavviso.

Il Delegato, a norma di quanto disposto dall'art. 28 let. h) (per analogia) e dell'art. 32 let. d) (per specifica previsione) GDPR 2016/679 dev'essere valutato almeno annualmente.

La medesima procedura di verifica è da applicarsi relativamente agli Amministratori di Sistema, come previsto dal Provvedimento del Garante del 27 novembre 2008 recepito in Gazzetta Ufficiale Nr. 300 del 24 dicembre 2008.

2.3.3 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti ai soggetti nominati in qualità di "Delegato Privacy" e "Delegato al trattamento" interno:

Codice	Tipo di documento	Descrizione
RDT	Lettera di nomina	Delegato Privacy
RST	Lettera di nomina	Delegato al trattamento interno
NOCD	Istruzioni	Norme Comportamentali Delegati

2.4 L'Incaricato al trattamento

2.4.1 La Figura base del sistema privacy: l'incaricato

Per la normativa vigente nazionale l'Incaricato è la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Delegato. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la loro diretta autorità, attenendosi alle istruzioni impartite.

La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Quando il trattamento si svolge con strumenti elettronici, è da intendersi quale misura di sicurezza l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.

Quando il trattamento si svolge senza l'ausilio di strumenti elettronici è da intendersi quale misura di sicurezza l'aggiornamento periodico dell'individuazione dell'ambito di trattamento consentito agli incaricati, la previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti, la previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e la disciplina delle modalità di accesso per identificare gli incaricati.

2.4.2 Nomina degli incaricati

La designazione degli incaricati deve essere espressa e specifica, da effettuarsi per iscritto e con riguardo a determinate mansioni (Rif. Mod. IDT2).

È parificata la preposizione della persona fisica ad una unità organizzativa per la quale sia individuato per iscritto l'ambito del trattamento consentito agli addetti preposti.

La designazione non ha natura contrattuale, ma di semplice conferimento di mansioni.

La lettera di incarico deve essere controfirmata per conoscenza.

Nella lettera di nomina devono essere precisati i trattamenti e le banche dati per le quali sono autorizzati a trattare i dati personali (Sistema di autorizzazione). Tale specifica potrà essere riportata in dettaglio, riportando i singoli trattamenti oppure richiamando lo specifico "Registro dei Trattamenti – Mappatura delle Aree e dei Ruoli Aziendali (DTEC_G)" ove sono riportati, per ciascun trattamento e per ciascun incaricato, gli accessi e i livelli di trattamento, sulla base della seguente tabella:

Classificazione dei Permessi consentiti alle operazioni di trattamento ex art. 4 GDPR 2016/679

A	Blocco, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Elaborazione, Estrazione, Interconnessione, Modificazione, Organizzazione, Raccolta, Raffronto, Registrazione, Selezione, Utilizzo
B	Cancellazione, Comunicazione, Conservazione, Consultazione, Elaborazione, Estrazione, Interconnessione, Modificazione, Organizzazione, Raccolta, Raffronto, Registrazione, Selezione, Utilizzo
C	Conservazione, Consultazione, Elaborazione, Estrazione, Interconnessione, Modificazione, Organizzazione, Raccolta, Raffronto, Registrazione, Selezione, Utilizzo
D	Conservazione, Consultazione, Selezione, Utilizzo
E	Conservazione, Consultazione
⊗	ACCESSO NEGATO

All'incaricato devono essere fornite le istruzioni operative alle quali attenersi nelle operazioni di trattamento e idonea formazione. La nomina è a tempo indeterminato. L'incaricato può essere revocato in ogni momento. L'incaricato deve attenersi, nel trattamento dei dati personali, alle istruzioni ricevute verbalmente, con la lettera d'incarico e con quanto previsto dalle Norme Comportamentali specifiche (NOCD/NOCI).

2.4.3 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti ai soggetti nominati in qualità di “Incaricato del trattamento” interno:

Codice	Tipo di documento	Descrizione
IDT2	Lettera di nomina	Incaricato del trattamento dei dati personali ex art. 30
DTEC_F	Registro	Registro dei Trattamenti – Elenco del Personale autorizzato al trattamento dei dati
DTEC_G	Registro	Registro dei Trattamenti – Mappatura delle Aree e dei Ruoli Aziendali
NOCI	Istruzioni	Norme Comportamentali Incaricati

2.5 Responsabile della protezione dei dati personali (RDP/DPO)

2.5.1 Nozione di Responsabile del trattamento di dati personali

I riferimenti normativi sulla figura del responsabile del trattamento, all'interno del GDPR 2016/679, sono riportati alla sezione IV articoli dal 37 al 39.

2.5.2 Requisiti

Il Responsabile della protezione dei dati, nominato dal Titolare del trattamento o dai suoi Delegati, dovrà:

a) Possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
b) Adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
c) Operare alle dipendenze del titolare o dei suoi delegati oppure sulla base di un contratto di servizio (RPD/DPO esterno).

Il Titolare o il Delegato privacy / Delegato al trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

2.5.3 In quali casi è previsto

Dovranno designare obbligatoriamente un RPD:

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

2.5.4 Quali sono i sui compiti

Il Responsabile della protezione dei dati è incaricato dei seguenti compiti:

a) attività di assistenza e consulenza professionale per le figure apicali dell'organizzazione aziendale nell'applicazione della disciplina prevista dal Regolamento UE 2016/679 (Rif. art. 39 c. 1a GDPR 2016/679);
b) attività di assistenza e consulenza per i lavoratori dell'organizzazione aziendale, che eseguono i trattamenti di dati personali (Rif. art. 39 c. 1a GDPR 2016/679);
c) attività di monitoraggio e vigilanza sulla corretta applicazione del GDPR da parte (Rif. art. 39 c. 1a GDPR 2016/679) (Rif. art. 39 c. 1b GDPR 2016/679). A tale fine si procederà:
    a. alla raccolta periodica di informazioni, per individuare eventuali nuovi trattamenti;
    b. all'analisi e verifica dei trattamenti in essere, nei termini di loro conformità al GDPR;
    c. allo svolgimento di attività di informazione, consulenza e indirizzo per il management;

   d. alla verifica in merito all'aggiornamento mensile del registro delle attività di trattamento ai sensi dell'articolo 30 del GDPR 2016/679;
   e. a fornire assistenza nella revisione della modulistica (informative, policy, ecc.;)alla revisione delle procedure interne all'organizzazione aziendale (regolamento privacy, videosorveglianza per finalità di sicurezza urbana, etc.);
   f. sorvegliare le politiche del Titolare del trattamento o del Responsabile del trattamento / Delegato privacy in materia di protezione dei dati personali in merito all'attribuzione delle responsabilità, alla sensibilizzazione alla formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   g. ad effettuare attività di audit.

d) ad assistere il Titolare nello svolgimento di attività d'impatto sulla protezione dei dati (c.d. D.P.I.A - Data Protection Impact Assessment) ai sensi dell'articolo 35 del GDPR 2016/679. Nello specifico si parteciperà alla valutazione dei nuovi progetti che presentano un impatto privacy. Ogni attività di D.P.I.A andrà documentata (Rif. art. 39 c. 1c GDPR 2016/679);
e) a fungere da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. (Rif. art. 39 c. 1d-e GDPR 2016/679).

Nell'eseguire i propri compiti il Responsabile della protezione dei dati dovrà considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Gli interessati potranno contattare il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali (eseguito da parte del Titolare, o del Responsabile del trattamento / Delegato privacy o delle persone autorizzate a trattarli), e all'esercizio dei loro diritti derivanti dal presente regolamento.

Periodicamente, e comunque nel momento in cui se ne ravvisi la necessità, il RPD relazionerà tempestivamente per iscritto agli organi apicali dell'azienda circa la conformità o le non conformità riscontrate, indicando, in tal caso, i correttivi ritenuti necessari.

La L'OFFICINA DELL'AIAS Coop. Soc., nella persona del proprio Titolare del trattamento, ha ritenuto, in data 24/05/2018, di non nominare un proprio RDP/DPO in quanto, fatte le opportune valutazioni, ritiene che non ricorrano nel suo caso le seguenti caratteristiche:

a) amministrazioni ed enti pubblici;
b) l'attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) l'attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Tale valutazione verrà verificata dal Titolare almeno annualmente.

2.6 Il Custode delle copie delle credenziali di autenticazione

2.6.1 Ruolo e Compiti del custode delle copie delle credenziali di autenticazione

Se ritenuta misura opportuna il Titolare, il Responsabile o il Delegato (se designato) possono nominare uno o più custodi delle credenziali di autenticazione.

Il custode è tenuto a:

- Conservare le credenziali di autenticazione degli incaricati del trattamento.
- Predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto.
- Istruire gli incaricati del trattamento sull'uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia.
- Revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali.
- Revocare le credenziali per l'accesso ai dati degli incaricati nel caso di mancato utilizzo per oltre 6 (sei) mesi.

Se la figura del custode non è nominata, la sua funzione è assunta dal un Delegato.

L'OFFICINA DELL'AIAS Coop. Soc. ha deciso di nominare Custode delle credenziali di autenticazione:

Cognome e Nome	Tipologia di servizio/credenziale
CERPELLONI CLAUDIO	Presidente Pro Tempore

2.6.2 Nomina del custode delle copie delle credenziali

La nomina del custode è soggetta alla stessa disciplina relativa alla nomina dell'incaricato (Vedi *supra § 2.4.2).* Rif. Mod. CDP.

2.6.3 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti ai soggetti nominati in qualità di "Incaricato della custodia delle copie delle credenziali":

Codice	Tipo di documento	Descrizione
CDP	Lettera di nomina	Incaricato della custodia delle copie delle credenziali

2.7 Il preposto alle copie di sicurezza delle banche dati

2.7.1 Ruolo e compiti del preposto alle copie di sicurezza delle banche dati

Il preposto alle copie di sicurezza delle banche dati è una persona fisica o giuridica che ha il compito di sovraintendere alla loro esecuzione periodica.

Spetta ad un Delegato individuare le figure interne od esterne preposte a questa attività di sicurezza.

Con idonea policy interna, il preposto alle copie di sicurezza delle banche dovrà prevedere:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta.
- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

I preposti a questa attività dovranno:

- Adottare tutte le prescrizioni opportune volte ad evitare la perdita, la distruzione e la cancellazione dei dati.
- Verificare lo status delle copie di sicurezza dei dati.
- Assicurarsi della conservazione delle copie di sicurezza in luogo idoneo e ad accesso controllato.
- Custodire con diligenza e perizia i dispositivi utilizzati per le copie di sicurezza.
- Riferire ogni informazione utile al Delegato al trattamento / Delegato privacy.

L'OFFICINA DELL'AIAS Coop. Soc. ha deciso di nominare Preposto alle copie di sicurezza delle banche dati:

Cognome e Nome	Tipologia di servizio/credenziale
GAMBIN FABIO	Direttore Economico Gestionale

2.7.2 Nomina del preposto

La nomina del preposto alla custodia delle copie di sicurezza è soggetta alla stessa disciplina relativa alla nomina dell'incaricato (Vedi *supra § 2.4.2).* Rif. Mod. BKP.

2.7.3 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti ai soggetti nominati in qualità di "Incaricato delle copie di sicurezza":

Codice	Tipo di documento	Descrizione
BKP	Lettera di nomina	Incaricato delle copie di sicurezza
ReB	Registro	Registro Backup

3 Trattamenti con strumenti elettronici

3.1 Sistema di autenticazione informatica

3.1.1 Procedura di identificazione

Nel caso in cui il trattamento di dati personali è effettuato con strumenti elettronici, il trattamento è consentito solamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

3.1.2 Identificazione dell'incaricato

Le credenziali di autenticazione possono consistere in:

- Un codice per l'identificazione dell'incaricato associato a una parola chiave riservata e conosciuta solamente dal medesimo.
- Un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave.
- Una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali devono essere disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni Incaricato del trattamento possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

3.1.3 Password

La componente riservata delle credenziali di autenticazione (parola chiave/password) deve rispettare i seguenti criteri (Rif. Mod. DTEC_S):

- Non deve contenere nomi comuni
- Non deve contenere nomi di persona
- Deve contenere sia lettere che numeri
- Deve comprendere almeno 3 caratteri alfabetici
- Deve comprendere almeno 2 caratteri numerici
- Deve essere diversa dallo User-Id
- Deve essere lunga 8 caratteri o massimo consentito dal sistema di autenticazione
- Non deve essere riconducibile all'incaricato.

Ogni incaricato deve essere informato e reso edotto che:

- Le credenziali di accesso sono personali
- Le credenziali di accesso devono essere memorizzate
- Le credenziali di accesso non devono essere comunicate a nessuno

- Le credenziali di accesso non devono essere trascritte

3.1.4 Regole comportamentali per assicurare la segretezza delle credenziali

Gli incaricati sono tenuti ad adottare la diligenza e la perizia opportuna al fine di garantire la segretezza della parola chiave**.**
Gli incaricati sono custodi dei dispositivi a loro affidati (badge magnetici, tessere magnetiche, ecc..).
È vietato comunicare a chiunque altro incaricato le proprie credenziali di accesso al sistema informatico.

3.1.5 Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico

Gli incaricati del trattamento hanno l'obbligo di:

- Non lasciare incustodito il proprio posto di lavoro.
- Di chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.

3.1.6 Accesso straordinario

Il preposto alla custodia delle copie delle credenziali, ha il dovere di consentire per esigenze organizzative, produttive e/o di sicurezza l'accesso ai dati e agli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato.

La custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza.

Il preposto alla custodia deve informare tempestivamente l'Incaricato di ogni accesso straordinario.

3.1.7 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti al Sistema di Autenticazione adottato:

Codice	Tipo di documento	Descrizione
DTEC_S	Modello	Criteri di assegnazione password nei sistemi di elaborazione
ReGP	Registro	Registro Gestione Password
SAI	Istruzioni	Sistema Autenticazione - istruzioni custodia password
SAIN	Istruzioni	Sistema Autenticazione - istruzioni custodia password - notebook
SAMP1	Modulo	Sistema Autenticazione - modulo prima consegna password
SAMP	Modulo	Sistema Autenticazione - modulo custodia password
SAN	Istruzioni	Sistema Autenticazione - note incaricato custodia pw

3.2 Sistema di autorizzazione

Il Titolare o il Delegato al trattamento / Delegato privacy se designato ha il compito di individuare gli Incaricati del trattamento per ogni tipologia di banca di dati personali trattata (Rif. Mod. DTEC_F).

Il tipo di trattamento effettuato da ogni singolo Incaricato del trattamento può essere differenziato.

Ogni Incaricato del trattamento può avere la possibilità di:

- Inserire nuove informazioni nella banca dati
- Accedere alle informazioni in visualizzazione e stampa
- Modificare le informazioni esistenti nella banca dati
- Cancellare le informazioni esistenti nella banca dati

L'elenco dei permessi deve essere costantemente aggiornato (Rif. Mod. DTEC_G).

3.2.1 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti al Sistema di Autorizzazione adottato:

Codice	Tipo di documento	Descrizione
DTEC_F	Modello	Personale autorizzato al trattamento dei dati
DTEC_G	Modello	Permessi di accesso ai dati

3.3 Ulteriori misure di sicurezza

Alla luce della disciplina in materia di data protection è vietato:

- Effettuare copie su supporti magnetici non autorizzati.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Delegato al trattamento / Delegato privacy i dati oggetto del trattamento.
- Consegnare a persone non autorizzate stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

3.3.1 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti alle ulteriori misure di sicurezza organizzatine dottate:

Codice	Tipo di documento	Descrizione
DTEC_O	Prescrizione	Modalità di protezione dei dati e dei locali
DTEC_P	Prescrizione	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

3.4 Aggiornamento e revisione del documento riepilogativo del sistema privacy

Con cadenza almeno annuale, il Titolare del trattamento o il Delegato Privacy su specifico incarico, deve aggiornare ed eventualmente predisporre una nuova versione del Documento Riepilogativo del Sistema Privacy contenente idonee informazioni riguardo al trattamento dei dati, all’applicazione delle misure minime e ad ogni altro adempimento previsto dalla normativa Privacy attualmente in vigore.

3.5 Censimento dei trattamenti di dati personali

3.5.1 Elenco delle sedi e degli uffici in cui vengono trattati i dati

Il Delegato al trattamento / Delegato privacy, se designato ha il compito di censire i trattamenti di dati personali effettuati dal Titolare nonché redigere e aggiornare l'elenco delle sedi in cui viene effettuato il trattamento dei dati (Rif. Mod. DTEC_B).

3.5.2 Elenco degli archivi dei dati oggetto del trattamento

Al Delegato al trattamento / Delegato privacy, se designato, è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati (Rif. Mod. DTEC_A). Ogni banca di dati o archivio deve essere classificato in relazione alle informazioni contenute indicando se si tratta di:

- Dati personali Identificativi
- Dati personali Sensibili
- Dati personali Giudiziari

3.5.3 Elenco dei sistemi di elaborazione per il trattamento

Il Delegato al trattamento / Delegato privacy, se designato, deve redigere e aggiornare una scheda riepilogativa del Sistema Informativo Aziendale (Rif. Mod. DTEC_C e DTEC_D). Per ogni sistema deve essere specificato:

- L'Incaricato della gestione e della manutenzione (Rif. Mod. GMSE).
- Il nome dell'incaricato o degli incaricati che lo utilizzano
- Il nome di uno o più preposti della custodia delle copie delle credenziali

L'OFFICINA DELL'AIAS Coop. Soc. ha deciso di nominare Incaricato della gestione e manutenzione degli strumenti elettronici:

Cognome e Nome	Tipologia di servizio/credenziale
GAMBIN FABIO	Direttore Economico Gestionale

3.5.4 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti alle Sedi, agli elenchi dei trattamenti aziendali (archivi) e alla Struttura del Sistema Informativo Aziendale:

Codice	Tipo di documento	Descrizione
GMSE	Lettera di nomina	Incaricato gestione e manutenzione strumenti elettronici
DTEC_A	Modello	Registro dei trattamenti e delle banche dati del Titolare
DTEC_B	Modello	Elenco delle sedi/uffici in cui vengono trattati i dati
DTEC_C	Modello	Scheda riepilogativa del Sistema informativo aziendale
DTEC_D	Modello	Sistemi di elaborazione per il trattamento dei dati

3.6 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

3.6.1 Elenco dei soggetti autorizzati al trattamento dei dati

Il Delegato al trattamento / Delegato privacy deve assegnare le credenziali di autenticazione e aggiornare l'elenco del personale autorizzato al trattamento dei dati (Rif. Mod. DTEC_J).

3.6.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

Il Delegato al trattamento / Delegato privacy ha il dovere di verificare, le credenziali di autenticazione e di aggiornare l'elenco dei soggetti autorizzati al trattamento dei dati.

3.6.3 ALLEGATI

Documento di riferimento, allegato al presente e debitamente compilato, contenente l'organigramma privacy adottato:

Codice	Tipo di documento	Descrizione
DTEC_J	Modello	Distribuzione dei compiti e delle responsabilità

3.7 Analisi dei rischi

3.7.1 Analisi dei rischi hardware

Il Titolare o il Delegato al trattamento / Delegato privacy se designato, anche avvalendosi di consulenti interni o esterni, deve di verificare ogni anno (Rif. Mod. DTEC_Z e RRAC):

- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati
- La situazione delle apparecchiature periferiche
- La situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito

3.7.2 Analisi dei rischi sui sistemi operativi e sui software installati

Il titolare o il Delegato al trattamento / Delegato privacy, se designato, deve verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei software utilizzati.
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

3.7.3 Analisi degli altri rischi nel trattamento dei dati

Il titolare o il Delegato al trattamento / Delegato privacy, se designato, deve analizzare eventuali altri rischi connessi al trattamento dei dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Rischi connessi al comportamento degli operatori

- Rischi connessi al contesto fisico ed ambientale

Per ogni altra indicazione di dettaglio, relativamente alla Valutazione Rischi, si rimanda alle specifiche schede sotto elencate. In particolare alla "DTEC_Z – Valutazione Rischi" ove sono state riportate, in dettaglio, la metodologia di valutazione, i criteri per l'individuazione e la valutazione dei rischi e le misure per la prevenzione e protezione dai rischi.

3.7.4 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti l'Analisi dei Rischi incombenti sui dati trattati:

Codice	Tipo di documento	Descrizione
DTEC_Z	Modello	DTEC_Z – Valutazione Rischi
RRAC	Registro	Registro dei Rischi e delle Azioni Correttive
SKRHW	Scheda	Scheda Rischio Hardware
SKRSW	Scheda	Scheda Rischio Software
SKRV	Scheda	Scheda Rilevazione contagio Virus

3.8 Misure da adottare per garantire l'integrità e la disponibilità dei dati

Il Titolare o il Delegato, se designato, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.
I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
Il "Documento con le istruzioni di copia" deve essere conservato a cura del Delegato in luogo sicuro e deve essere trasmesso in copia controllata a ciascun incaricato delle copie di sicurezza delle banche dati (Rif. Mod. DTEC_M).

In particolare per ogni banca di dati debbono essere definite le seguenti specifiche:

- Il Tipo di supporto da utilizzare per le Copie di sicurezza dei dati.
- Il numero di Copie di sicurezza dei dati effettuate ogni volta
- Se i supporti utilizzati per le Copie di sicurezza dei dati sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le Copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle Copie di sicurezza dei dati.
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- Il nome dell'incaricato a cui è stato assegnato il compito di effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare il ripristino delle Copie di sicurezza dei dati.

3.8.1 Attività di verifica e controllo del Sistema Informatico

In merito all'attività di controllo e verifica del Sistema Informativo Aziendale si rimanda a quanto disposto al cap. 3.13.1 del presente manuale.

3.8.2 ALLEGATI

Documento di riferimento, allegato al presente e debitamente compilato, contenente le procedure adottate per garantire l'integrità dei dati personali trattati mediante elaboratori elettronici:

Codice	Tipo di documento	Descrizione
DTEC_M	Modello	Criteri e procedure per garantire l'integrità dei dati informatici

3.9 Misure da adottare per la protezione delle aree e dei locali

3.9.1 Misure generali

Di seguito vengono indicate regole procedurali per garantire la protezione degli ambienti in cui avvengono le operazioni di trattamento, in ossequio a quanto previsto dal Codice privacy e dal regolamento tecnico in materia di misure di sicurezza di tipo fisico (Rif. Mod. DTEC_O).

3.9.2 Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Il Titolare o il Delegato al trattamento / Delegato privacy se nominato deve redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati. Inoltre, deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati (Rif. Mod. RAL_LCC).

Per ulteriori e specifiche disposizioni si deve far riferimento a quanto previsto dalla scheda DTEC_O.

3.9.3 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti le modalità e le procedure di protezione delle aree e dei locali ove avviene il trattamento dei dati:

Codice	Tipo di documento	Descrizione
DTEC_O	Prescrizione	Modalità di protezione dei dati e dei locali
RAL_LCC	Lettera di consegna	Controllo degli accessi alle aree ai locali e consegna chiavi

3.10 Formazione degli incaricati del trattamento

3.10.1 Piano di formazione

Il Responsabile dell'Ufficio Legale, deve predisporre un adeguato piano di formazione interna per tutti i Delegati e gli incaricati (Rif. Mod. DTEC_H_N).

La formazione è programmata già al momento dell'ingresso in servizio di nuovi incaricati del trattamento, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il Piano di formazione del personale deve essere predisposto, per:

- Rendere edotti gli incaricati del trattamento sui rischi che incombono sui dati
- Rendere edotti gli incaricati del trattamento sulle misure disponibili per prevenire eventi dannosi
- Rendere edotti gli incaricati del trattamento sulle responsabilità che ne derivano
- Rendere edotti gli incaricati del trattamento sulle modalità per aggiornarsi sulle misure minime adottate dal titolare

Al momento dell'erogazione della Formazione dev'essere debitamente compilato un elenco del personale formato e dato riscontro al RDT e all'eventuale Responsabile interno Qualità.

3.10.2 ALLEGATI

Documento di riferimento, allegato al presente e debitamente compilato, contenenti il piano di formazione adottato ed il materiale formativo di base da utilizzarsi nelle sessioni di formazione:

Codice	Tipo di documento	Descrizione
DTEC_H_N	Modello	Piano di formazione del personale autorizzato al trattamento dei dati
ALL. 7.1	Slide	Corso Privacy per Incaricati.pptx
ALL. 7.1	Slide	Slide Misure Tecniche e Data Breach.ppt
ALL. 7.1	Guida	Guida al nuovo Regolamento europeo in materia di protezione dati.pdf
ALL. 7.1	Normativa	Normativa a tutela della protezione dei dati (GDPR 2016-679.pdf)
ALL. 7.1	Normativa	Normativa a tutela della protezione dei dati (DLGS196.pdf)
ALL. 7.1	Normativa	Normativa a tutela della protezione dei dati (DLGS196 - ALLB.pdf)

3.11 Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

3.11.1 Trattamenti di dati personali affidati all'esterno della struttura del titolare

Il Titolare, può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare. In questo caso, deve (anche tramite il Delegato) redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:

- I soggetti interessati
- I luoghi dove fisicamente avviene il trattamento dei dati stessi
- I responsabili del trattamento di dati personali

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, sia possibile nominare responsabili del trattamento soggetti controllabili dal Titolare del trattamento stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), è possibile nominarli Responsabili esterni.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, non sia possibile nominare i responsabili del trattamento, in quanto soggetti autonomi non controllabili dal titolare del trattamento stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), è possibile specificarne la titolarità (o co-titolarità) con specifiche clausole contrattuali.

3.11.2 Criteri per la scelta degli enti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare

Il Titolare del Trattamento, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti individuati dall'art. 28 del GDPR 2016/679 (*rif. supra § 2.2*).

3.11.3 Designazione del Responsabile del trattamento esterno

L'Addendum Privacy del responsabile esterno deve essere sottoscritto per accettazione.
Il Titolare deve informare il Responsabile del trattamento esterno, dei compiti che gli sono assegnati.

3.11.4 Designazione del titolare autonomo del trattamento in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Titolare, per tramite del Responsabile se designato deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno (Rif. Mod. DTEC_W_W2 e DTEC_E). La Titolarità del soggetto esterno deve risultare dal rapporto contrattuale o in mancanza di una dichiarazione di accettazione della qualifica di Titolare Autonomo. In questo caso al momento dell'affidamento dell'incarico il Titolare autonomo del trattamento in outsourcing, deve dichiarare per iscritto:

- Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali
- Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali
- Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
- Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
- Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

L'OFFICINA DELL'AIAS Coop. Soc. ha deciso di designare Responsabili Esterni del trattamento dei dati ex art. 28 GDPR 2016/679

Responsabile Esterno	Tipologia di servizio
EMME PARTNERS	Commercialista
STUDIO NODARI	Consulente del Lavoro e Paghe
ISO ENGINEERING SRL	Consulente per la Sicurezza sul Lavoro ex DLgs 81/08
BERNINI Dott. VITTORE	Medico del Lavoro
PERUSI Avv. STEFANO	Studio Legale
ISO ENGINEERING SRL	Consulente Certificazione in Qualità ISO 9001:2008
EMMANUEL Soc. Coop.	Cooperativa per l'assistenza in ATI
IL FOCOLARE Soc. Coop.	Cooperativa per l'assistenza in ATI
ISO ENGINEERING SRL	Consulente Privacy ex GDPR 2016/679

3.11.5 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti ai soggetti nominati in qualità di "Responsabile del trattamento" esterno (Out-sourcing):

Codice	Tipo di documento	Descrizione
DTEC_E	Modello	Enti terzi a cui è affidato il trattamento dei dati in out-sourcing
DTEC_W_W2	Addendum Privacy	Responsabile esterno al trattamento dei dati ex art. 28 GDPR 2016/679

3.12 Ulteriori misure

3.12.1 Protezione contro l'accesso abusivo

Il Titolare o il Delegato al trattamento / Delegato privacy, se designato, definisce, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione da parte di hackers su ogni sistema.

Per ogni sistema interessato debbono essere definite le seguenti specifiche:

- Le misure applicate per evitare intrusioni.
- Le misure applicate per evitare contagi da "Virus Informatici".

3.12.2 Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Per ogni banca di dati deve essere individuato il luogo di conservazione copie dei dati in modo che sia convenientemente protetto dai potenziali rischi di:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni e atti vandalici
- Incendio
- Allagamento
- Furto

Per ulteriori e specifiche disposizioni si deve far riferimento a quanto previsto dalla scheda DTEC_P.

3.12.3 Riutilizzo dei supporti rimovibili

Se il Titolare decide che i supporti magnetici contenenti dati sensibili o giudiziari non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.

E' compito del Delegato, se designato, assicurarsi che in nessun caso vengano lasciate copie di Banche di dati contenenti dati personali, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

Per ulteriori e specifiche disposizioni si deve far riferimento a quanto previsto dalla scheda DTEC_P.

3.12.4 Ripristino dell'accesso ai dati in caso di danneggiamento

La decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del Titolare o del Delegato, se designato.

3.13 Misure di tutela e garanzia

3.13.1 Descrizione degli interventi effettuati da soggetti esterni

Nel caso in cui ci si avvale di soggetti esterni alla propria struttura, per provvedere al controllo del buon funzionamento hardware e/o software degli strumenti elettronici e alla eventuale riparazione, aggiornamento o sostituzione, il Delegato deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta con la descrizione dettagliata delle operazioni eseguite che attesti la conformità a quanto stabilito dalla normativa a tutela della protezione dei dati (GDPR 2016/679 e normativa nazionale vigente).

4 Trattamenti senza l'ausilio di strumenti elettronici

4.1 Nomina e istruzioni agli incaricati

Per ogni archivio il Titolare o il Delegato, se designato, deve definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso negli archivi (Rif. Mod. DTEC_F, DTEC_J e DTEC_Q).
Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni. Per ulteriori e specifiche disposizioni si deve far riferimento a quanto previsto dalle schede DTEC_O, DTEC_P e DTEC_Q.

Qualora i documenti contengano dati sensibili o giudiziari ai sensi di quanto stabilito dalla normativa a tutela della protezione dei dati (GDPR 2016/679 e normativa nazionale vigente), gli incaricati del trattamento sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso all'Azienda, da parte sia del Personale che dei Terzi, può avvenire solo sulla base delle disposizioni di cui alla scheda DTEC_Q e, comunque, previa identificazione e registrazione dei soggetti (Rif. Mod. ReAL-1) da parte dell'eventuale Personale di Reception.

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti (Rif. Mod. ReAL-2).

Ulteriori disposizioni ed istruzioni, sia la Personale incaricato che delegato, sono riportate nella seguente documentazione:

NOCI – Norme comportamentali per il personale incaricato

ai quali si fa specifico riferimento. Tali istruzioni dovranno essere portate a conoscenza del Personale al momento dell'assunzione in Azienda e/o d'inizio attività. Inoltre dovranno essere appesi alla bacheca informativa aziendale ed essere disponibili attraverso una specifica cartella condivisa su server e/o nella intranet aziendale.

4.1.1 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti relativi alle misure e procedure per la protezione dei dati, nei trattamenti senza l'ausilio di strumenti elettronici (trattamenti cartacei):

Codice	Tipo di documento	Descrizione
DTEC_F	Modello	Personale autorizzato al trattamento dei dati
DTEC_J	Modello	Distribuzione dei compiti e delle responsabilità
DTEC_O	Modello	Modalità di protezione dei dati e dei locali
DTEC_P	Modello	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
DTEC_Q	Prescrizione	Modalità di trattamento senza l'ausilio di strumenti elettronici
ReAL-1	Registro	Registro Accesso Locali
ReAL-2	Registro	Registro Accesso Locali dopo l'orario di chiusura
NOCI	Istruzioni	Norme comportamentali

4.2 Copie degli atti e dei documenti

È fatto divieto a chiunque di:

- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Titolare o dal Delegato se designato di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

Per ulteriori e specifiche disposizioni si deve far riferimento a quanto previsto dalla scheda DTEC_Q.

4.3 Carico/Scarico dei documenti

In merito alla documentazione cartacea contenente dati personali sensibili e giudiziari è bene se ne mantenga traccia nella movimentazione aziendale, almeno riguardo all'entrata (carico) e all'uscita (scarico) dall'Azienda. Tali limiti temporali ne determinano la responsabilità, da parte dell'Azienda sul trattamento della medesima documentazione.
A tal fine si ritiene opportuno utilizzare un apposito registro di carico/scarico dei documenti (ReCSD) da utilizzare da parte del Personale Incaricato (ad es. la Reception, l'Amministrazione, etc.).

4.3.1 ALLEGATI

Codice	Tipo di documento	Descrizione
ReCSD	Registro	Registro Carico Scarico documenti

4.4 Distruzione dei documenti

Lo scarto rappresenta lo strumento per gestire in maniera ordinata un archivio corrente e di deposito: esso è un elemento qualificante dell'archivio stesso, in quanto permette di conservare solo ciò che, terminato il periodo di valenza amministrativa e legale, ha assunto un valore storico e consente di eliminare la documentazione giudicata superflua, che ha poco o niente da dire circa la storia e le competenze di un'istituzione, pubblica o privata che sia.
I tempi di conservazione dei documenti cartacei sono regolati, sulla base della specificità del documento medesimo, dalla normativa amministrativo-contabile, storica ed archivistica vigente.
Decorso il periodo obbligatorio di conservazione della documentazione, contenente dati personali, presso l'archivio aziendale i documenti, opportunamente selezionati sulla base della effettività validità ed importanza (ad es. non saranno oggetto di distruzione i documenti oggetto di procedimento giudiziale pluriennale in corso), dovranno essere condotti al macero previa loro distruzione mediane distruggidocumenti almeno di layer 2. L'alternativa è l'affido ad una società specializzata.
In ogni caso vi è la necessità di compilare il Registro Distruzione documenti (ReDD) riportante i singoli documenti/fascicoli avviati al macero. Inoltre è necessario stilare un verbale, in carta semplice, riepilogativo degli adempimenti eseguiti.
In caso di affido ad una società specializzata è necessario farsi rilasciare una lista di dettaglio di quanto prelevato ed un verbale di avvenuta effettiva distruzione.

4.4.1 ALLEGATI

Codice	Tipo di documento	Descrizione
ReDD	Registro	ReDD Registro Distruzione documenti

5 Diritti dell'interessato

5.1 Diritto di accesso ai dati personali (Art. 15 GDPR 2016/679)

Diritto di accesso dell'interessato

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

5.2 Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

5.3 Diritto alla cancellazione

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

5.4 Diritto di limitazione al trattamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3 L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

5.5 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

5.6 Diritto di opposizione

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

6 Amministratori di Sistema

6.1 Provvedimenti e modelli

In data 27 novembre 2008 il Garante per la protezione dei dati personali ha provveduto ad emanare un Provvedimento, recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008, relativo a "misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema". E' poi ritornato in argomento con i provvedimenti del 12 febbraio 2009 (G.U. n. 45 del 24 febbraio 2009) con cui si è disposto di unificare e contestualmente prorogare i termini per l'adempimento delle prescrizioni di cui al citato Provvedimento procrastinandone la scadenza al 30 giugno 2009; del 21 aprile 2009, con cui si è deciso di attivare una consultazione pubblica volta ad acquisire osservazioni e commenti da parte dei titolari del trattamento ai quali il provvedimento si rivolge con esclusivo riferimento a quanto prescritto al punto 2 del Provvedimento, dando tempo fino al 31 maggio 2009 per far pervenire osservazioni e commenti, pubblicato sulla G.U. n. 105 dell'8 maggio 2009; ed infine del 26 giugno 2009 con cui apportava modifiche al provvedimento del 27 novembre 2008 e proroga dei termini per il loro adempimento - 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009)

Vediamo più nel dettaglio cosa comportano questi provvedimenti in termini operativi nella gestione della protezione dei dati personali.

Quanto previsto dal Provvedimento del Garante, datato 27 novembre 2008 e sue successive modificazioni ed integrazioni, non si esaurisce nella mera predisposizione di una nuova lettera di incarico o nella modifica di quella già esistente ma richiede al titolare una serie di "misure e accorgimenti" e, non ultimi, di "adempimenti in ordine all'esercizio dei doveri di controllo da parte del titolare (***due diligence***)" sulle attività dell'amministratore.

6.1.1 L'adempimento in sintesi

Con il **provvedimento a carattere generale del 27 novembre 2008** dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008, il Garante per la protezione dei dati personali impone ai titolari di trattamenti di dati personali (anche solo in parte gestiti mediante strumenti elettronici) di predisporre un "elenco degli amministratori di sistema e loro caratteristiche".

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel Documento Riepilogativo del Sistema Privacy, oppure, nei casi in cui il titolare non sia tenuto a redigere il DPS, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Nella pratica occorre:

- **individuare coloro che ricadono nella categoria di "amministratore di sistema"**
- **valutare l'esperienza, la capacità e l'affidabilità** dei soggetti designati quali "amministratore di sistema" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza
- **designare tali "amministratore di sistema" in modo individuale** con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato
- **verificare l'operato degli amministratori di sistema, con cadenza almeno annuale**, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti
- **registrare gli accessi ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema**, mediante l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica).

Sono esclusi dall'ambito applicativo del presente provvedimento i titolari di alcuni trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili, i quali pongono minori rischi per gli interessati e sono stati pertanto oggetto di recenti misure di semplificazione (art. 29 D.l. 25 giugno 2008, n. 112, convertito, con modifiche, con Legge 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008).

6.1.2 Cosa si intende per amministratore di sistema?

Il primo punto di riflessione riguarda l'individuazione di coloro che ricadono nella categoria di "amministratore di sistema".

Tale figura, anche se non esplicitamente indicata nel "Codice in materia di protezione dei dati personali" era prevista, viceversa, dal DPR 318/1999 (abrogato dal Codice) che definisce l'amministratore di sistema il "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c).

Nel provvedimento del 27 novembre 2008 il Garante dice che con "amministratore di sistema" si individuano figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e che sono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli **amministratori di basi di dati**, gli **amministratori di reti** e di **apparati di sicurezza** e gli **amministratori di sistemi software complessi** e ciò anche quando l'amministratore non consulti "in chiaro" le informazioni relative ai trattamenti di dati personali.

6.1.3 Come si valutano le capacità dell'amministratore di sistema?

Il titolare, prima di procedere alla nomina, deve valutare l'esperienza, la capacità e l'affidabilità dei soggetti designati quali "amministratore di sistema" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

In che modo ciò può essere svolto (ed eventualmente dimostrato al Garante in caso di ispezione)?

È ovvio che si parte dal presupposto che chi di fatto svolge già oggi la funzione di amministratore di sistema sia in grado si svolgere la propria funzione; è opportuno allora predisporre una sorta di **curriculum vitae** di ciascun amministratore che indichi chiaramente titoli di studio, certificazioni professionali, esperienze professionali, corsi di formazione già svolti. Il CV deve essere datato e firmato sia dall'amministratore che dal titolare. L'indicazione dei percorsi formativi svolti specie per gli ambiti non prettamente tecnologici ma relativi invece alle problematiche della privacy e della protezione dei dati personali assume un valore particolarmente importante per il "rispetto della garanzia delle vigenti disposizioni". L'amministratore di sistema non può essere solo un bravo tecnico ma deve conoscere la normativa sulla privacy.

6.1.4 Cos'è una "due diligence"?

Il Garante nel provvedimento del 27 novembre 2008 sull'amministratore di sistema usa per la prima volta l'espressione "*due diligence*" per indicare "gli accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare" in relazione alle mansioni svolte dagli amministratori di sistema. Come è noto, nell'ambito dell'internal audit e dell'information security con "*due diligence*" si intende un'attività di analisi e verifica volta al raggiungimento di un parere di conformità (*compliance*) in relazione a particolari attività anche in relazione ai possibili rischi ed ai relativi impatti. Caratteristica della "due diligence" è inoltre, a fronte dei risultati ottenuti, la predisposizione di un piano di (eventuali) azioni correttive.

In sintesi l'output della *due diligence* del titolare sull'amministratore di sistema deve consistere almeno nei seguenti elementi:

1. giudizio di conformità sugli adempimenti richiesti;
2. valutazione dei possibili rischi (e relativi impatti);
3. indicazioni dei possibili interventi (se necessari o opportuni).

6.1.5 Designazione dell'amministratore di sistema

Occorre predisporre una lettera di "incarico" (Rif. Mod. ADSIN e ADSRE) specifica che contenga:

- attestazione che l'incaricato ha le caratteristiche richieste dalla legge;
- elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato;
- indicazione delle "verifiche" almeno annuali che il titolare svolgerà sulle attività svolte dall'amministratore di sistema;
- indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed
- eventualmente a terzi nei modi richiesti dalla legge.

L'OFFICINA DELL'AIAS Coop. Soc. ha deciso di nominare Amministratori di Sistema per l'anno 2020 i seguenti soggetti:

Amministratore di Sistema interno:

Fatte le opportune verifiche sul personale interno, soprattutto riguardo ai profili personali di competenza tecnica, imprescindibili ai fini di nomina, si ritiene di non procedere all'identificazione dell'Amministratore di Sistema Interno per l'anno in corso. Tale misura sarà oggetto di verifica con cadenza annuale in sede di revisione ed aggiornamento del Documento Riepilogativo del Sistema Privacy.

Responsabili esterni nel trattamento dei dati informatici:

- Fornitura, configurazione, manutenzione, aggiornamento, assistenza sistemi hardware (elaboratori elettronici, apparati di networking, sistemi serventi, etc.), soluzioni software sistemistiche e office-line;

RUN CONSULTING di Cortese Federico con sede in Via C. Colombo, 4 - 37026 Pescantina (VR)
Tel. +39 045 2820375 – eM.: federico@runconsulting.it

- Fornitura, configurazione, manutenzione, aggiornamento, assistenza soluzioni software gestionali di produzione e/o commercializzazione propria (*ADHOC REVOLUTION*)

ZUCCHETTI SPA con sede in Via Giovanni Cittadella, 7 - 35137 Padova (PD)
Tel. +39 0371 594-1 – eM.: admin@zucchettisoftware.it

6.1.6 Giudizio di conformità sugli adempimenti richiesti

Il giudizio di conformità viene realizzato dal titolare o da una terza parte indipendente rispetto ai sistemi informativi (ad esempio l'Internal Audit) mediante la verifica del rispetto degli adempimenti richiesti.

A riguardo può essere utile utilizzare una "check list di controllo" appositamente predisposta (v. p. 6.3 del presente documento).

6.1.7 ALLEGATI

Documenti di riferimento, allegati al presente e debitamente compilati, contenenti tutti i riferimenti relativi alle nomine degli Amministratori di Sistema e dei Responsabili Esterni nel trattamento dei dati informatici, sono:

Codice	Tipo di documento	Descrizione
ADSVN	Verbale	Verbale di nomina degli ADS

ADSVV	Verbale	Verbale annuale di verifica degli ADS
ADSEL	Modello	Elenco degli ADS
ADSCD	Modello	Comunicazione Dipendenti
ADSIN	Lettera	Lettera di nomina ADS Interno
ADSRE	Addendum Privacy	Addendum Privacy Responsabile Esterno nel trattamento di dati informatici
ADSRN	Lettera	Richiesta nominativi
ADSIDT2	Lettera	Lettera Incarico Trattamento - Stagista Tecnico
ADSIN2	Lettera	Lettera Incarico ADS Tecnico incaricato interno

6.2 Riepilogo degli adempimenti richiesti:

1) **nominare gli amministratori di sistema, siano essi interni o esterni**. E' meglio accompagnare la nomina con un documento in cui si inquadrino responsabilità e ambiti di azione:

   1.a) **Valutazione delle caratteristiche soggettive**: in sostanza, si devono nominare amministratori di sistema persone con adeguata esperienza, capacità e affidabilità.
   1.b) **Designazioni individuali**: la nomina deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Questo è un concetto molto importante, perché oltre alla nomina dei responsabili e degli incaricati adesso occorrerà nominare anche gli amministratori, tramite una lettera di incarico in cui si dovranno indicare anche le rispettive mansioni e gli ambiti di intervento.
   1.c) **Servizi in outsourcing**: nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Anche in questo frangente l'adempimento è più rilevante che in passato, visto che per nel caso di responsabili di trattamenti in outsourcing il titolare era tenuto alla semplice nomina del responsabile esterno, senza ricevere informazioni sugli incaricati da esso designati. In pratica, non si trattavano nominativi di appartenenti a società esterne, mentre ora devono essere ben registrati. Se si erogano servizi informatici, hardware e/o software, di qualunque tipo e/o livello l'Azienda deve comunicare, almeno annualmente, i nominativi dei tecnici preposti ai propri Clienti.

2) **riportare l'elenco degli amministratori di sistema nel DRSP**.

   2.a) **Elenco degli amministratori di sistema**: gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel Documento Riepilogativo del Sistema Privacy. Questo è una novità rispetto alle nomine precedenti di incaricati e responsabili, che non dovevano essere inserite nel DRSP. A questo proposito, si consiglia di riportate questo elenco in uno degli allegati al DRSP, per motivi di protezione dei dati personali degli amministratori stessi. Inoltre, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti.

3) Se si erogano servizi informatici, hardware e/o software, di qualunque tipo e/o livello l'Azienda deve **notificare l'elenco nominativo degli amministratori di sistema interni e le ragioni sociali degli amministratori di sistema esterni**, almeno annualmente, intesi come nominativi dei tecnici preposti ai propri Clienti

4) **notificare l'elenco degli amministratori di sistema ai dipendenti tramite informativa** (si può fare in diversi modi, dalla notifica al momento della nomina come incaricati del trattamento ad una schermata informativa in fase di login al sistema, oppure con una circolare in bacheca o una mail rivolta a tutti);

5) **verificare periodicamente l'operato degli amministratori di sistema e i nominativi previsti** (questo si può anche fare annualmente, in fase di revisione del DRSP)

5.a) **Verifica delle attività:** l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

6) **attuare la registrazione temporale degli accessi al sistema da parte degli amministratori**. Questo è comunque un argomento che va studiato caso per caso.

6.a) **Registrazione degli accessi:** devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le 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. Questo è un adempimento piuttosto complesso da rispettare, poiché è richiesto il tracciamento degli accessi degli amministratori al sistema informatico in termini di riferimenti temporali. Ma se la cosa è fattibile per quanto riguarda i sistemi operativi (es accesso ai sistemi windows), non è detto che gli applicativi specifici (es ragioneria, paghe, etc.) siano in grado di tracciare tali log. Inoltre, la cosa diventa ulteriormente complessa nei casi in cui gli archivi vengano gestiti con strumenti di office automation: se ad esempio un archivio è gestito con un foglio excel, registrare tutti gli accessi diventa nel complesso di difficile gestione.

6.3 Check-up tipo di valutazione, ad uso degli Amministratori di Sistema

Giudizio di conformità sugli adempimenti richiesti
(Fonte: compliancenet.it)

Obiettivi di controllo	*Presidio*	*Verifica effettuata*	*Grado di conformità*
Censimento dei trattamenti			
Tutti i trattamenti di dati personali effettuati (anche in parte) mediante strumenti elettronici sono censiti e sono indicati i relativi "amministratori di sistema".	Il regolamento aziendale XX prevede che l'inizio di qualsiasi nuovo trattamento di dati personali sia comunicato al delegato privacy che provvede ad aggiornare il censimento dei trattamenti	È stata presa visione dell'ultimo censimento dei trattamenti disponibile presso il delegato privacy e verificato che fosse completo.	1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
Se i trattamenti sono affidati	Nei contratti di outsourcing	È stata presa visione degli	1) Conforme _____

a terze parti queste hanno comunicato al Titolare l'elenco dei relativi "amministratori di sistema".	sono inserite clausole specifiche a riguardo. Almeno una volta l'anno viene richiesto l'aggiornamento della lista degli amministratori di sistema	elenchi forniti dagli *outsourcer*.	2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
Se il trattamento comprende, "anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori" è stata resa nota e conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni.	L'informativa ai dipendenti prevede tale comunicazione. L'ufficio Formazione cura attraverso la intranet aziendale gli aggiornamenti al personale relativi a tale adempimento.	È stata presa visione delle lettere di incarico. È stata consultata la intranet per verificare la presenza di tali comunicazioni.	1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
Lettera di incarico			
Per ogni "amministratore di sistema" è disponibile la lettera di incarico comprendente (al minimo):	Esiste uno standard di lettera di incarico ad "amministratore di sistema" che prevede le caratteristiche richieste dalla legge.	È stata acquisita copia dello standard.	
☐ attestazione che l'incaricato ha le caratteristiche richieste dalla legge;			
☐ elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato;			1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
☐ indicazione delle "verifiche" almeno annuali che il titolare svolgerà sulle attività svolte dall'amministratore di sistema;			1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
☐ indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed			1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____

eventualmente a terzi nei modi richiesti dalla legge.			4) Non applicabile ___ Note (per 3 o 4): _____
<u>Elenco degli amministratori</u>			
Gli estremi identificativi delle persone fisiche nominate "amministratori di sistema", con l'elenco delle funzioni ad essi attribuite, sono stati riportati nel Documento Riepilogativo del Sistema Privacy, oppure, nei casi in cui il titolare non sia tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.	È stato predisposto un "elenco degli amministratori" ed allegato al Documento Riepilogativo del Sistema Privacy.	È stato acquisito il DPS e l'allegato relativo all'elenco degli amministratori	1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
<u>Registrazione degli accessi</u>			
È adottato un idoneo sistema per la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.	In azienda è in uso il **sistema ABC** di gestione degli accessi logici; tale sistema prevede il log degli accessi.	È stata presa visione del sistema ABC e del manuale che ne descrive le caratteristiche	1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
Tali registrazioni (*access log*) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.	Il log degli accessi relativi agli amministratori di sistema è protetto con credenziali specifiche che sono custodite dal Direttore Generale in busta sigillata dentro una cassaforte. Il DG non è a conoscenza delle credenziali. In caso di necessità le credenziali sono date in uso al personale tecnico e poi modificate e nuovamente assegnate al Direttore Generale. Il **sistema ABC** di gestione dei log mantiene copia inalterabile dei log.	È stata presa visione delle credenziali riservate custodite dal Direttore Generale. È stata presa visione del sistema ABC e del manuale che ne descrive le caratteristiche.	1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
Le registrazioni comprendono i riferimenti	I log sono conservati per sei mesi.	Sono stati visionati i log.	1) Conforme _____ 2) Non conforme

temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi.			___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
Verifiche del titolare			
L'operato degli amministratori di sistema è verificato, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.	Annualmente, in occasione dell'aggiornamento del Documento Riepilogativo del Sistema Privacy, viene verificato il rispetto degli obblighi normativi relativi all'amministratore di sistema.	È stata compilata la presente check list in occasione dell'aggiornamento del DPS:	1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____
Per i trattamenti affidati a terze parti, queste hanno attestato per iscritto di aver effettuato, con cadenza almeno annuale, le verifiche sui relativi amministratori di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.	Annualmente, in occasione dell'aggiornamento del Documento Riepilogativo del Sistema Privacy, viene richiesta alle terze parti che hanno in *outsourcing* trattamenti di dati personali dell'azienda, l'attestazione sulle verifiche del rispetto degli obblighi normativi relativi all'amministratore di sistema.	Sono state visionate le attestazioni da parte degli *outsourcer.*	1) Conforme _____ 2) Non conforme ___ 3) Parzialmente conforme _____ 4) Non applicabile ___ Note (per 3 o 4): _____

Valutazione dei possibili rischi (e relativi impatti)

Obiettivi di controllo	*Grado di conformità*	*Note sul grado di conformità*	*Rischi*	*Impatti*
Censimento dei trattamenti	Conforme			
Lettera di incarico	Conforme			
Elenco degli amministratori	Parzialmente conforme	Mancano le liste relative a due società terze nominate responsabili del trattamento.	Rischio di accesso non autorizzato Rischio di trattamento non consentito o non conforme alle finalità della raccolta	sanzione da 20.000 a 120.000 euro
Registrazione degli accessi	Parzialmente conforme	Tecnicamente non si ha evidenza del fatto che i log non siano effettivamente modificabili.	Rischio di distruzione o perdita, anche accidentale, dei dati Rischio di accesso non autorizzato Rischio di trattamento non consentito o non conforme alle finalità della raccolta	sanzione da 20.000 a 120.000 euro
Verifiche del titolare	Parzialmente conforme	Non esistono piani di formazione volti ad un costante aggiornamento degli amministratori di sistema in relazione agli adempimenti di legge.	Mancata adozione di misure minime di sicurezza	sanzione da 20.000 a 120.000 euro

Indicazioni dei possibili interventi (se necessari o opportuni)

Obiettivi di controllo	*Note sul grado di conformità*	*Azione*	*Data di completamento*	*In carico a*
Elenco degli amministratori	Mancano le liste relative a due società terze nominate responsabili del trattamento.	Ottenere le liste mancanti. Disdire il contratto in mancanza delle liste entro 30 giorni.	1 giugno 2009	Ufficio Legale
Registrazione degli accessi	Tecnicamente non si ha evidenza del fatto che i log non siano effettivamente modificabili	Individuare una soluzione che garantisca l'immodificabilità dei log.	30 luglio 2009	Sistemi informativi
Verifiche del titolare	Non esistono piani di formazione volti ad un costante aggiornamento degli amministratori di sistema in relazione agli adempimenti di legge	Aggiornare il piano di formazione degli amministratori di sistema.	15 aprile 2009	Ufficio Formazione

7 Regolamenti, Disciplinari e Formazione

7.1 Formazione

Relativamente alla formazione del Personale, sia esso Incaricato che Delegato, di ogni ordine e grado si rimanda a quanto previsto al capitolo 3.10 del presente manuale. Qui si ricorda solo che i supporti formativi a disposizione risultano i seguenti:

Codice	Tipo di documento	Descrizione
DTEC_H_N	Modello	Piano di formazione del personale autorizzato al trattamento dei dati
ALL. 7.1	Slide	Corso Privacy per Incaricati.pptx
ALL. 7.1	Slide	Slide Misure Tecniche e Data Breach.ppt
ALL. 7.1	Guida	Guida al nuovo Regolamento europeo in materia di protezione dati.pdf
ALL. 7.1	Normativa	Normativa a tutela della protezione dei dati (GDPR 2016-679.pdf)
ALL. 7.1	Normativa	Normativa a tutela della protezione dei dati (DLGS196.pdf)
ALL. 7.1	Normativa	Normativa a tutela della protezione dei dati (DLGS196 - ALLB.pdf)

Tali supporti formativi saranno gestiti e aggiornati dal Delegato Privacy Aziendale, coadiuvato dalle eventuali altre professionalità necessarie presenti in Azienda e/o di Consulenza esterna.

7.2 Istruzioni agli incaricati

Le istruzioni specifiche destinate al Personale destinato al trattamento dei dati personali sono riportate, oltre che sulle singole lettere d'incarico, anche nei seguenti documenti:

Codice	Tipo di documento	Descrizione
NOCD	Prescrizioni	Norme comportamentali per Delegati
NOCI	Prescrizioni	Norme comportamentali per Incaricati

Le lettere d'incarico (IDT2), contenenti tali norme comportamentali, devono essere consegnate a ciascun dipendente incaricato e/o delegato e fatte sottoscrivere.

Tali norme comportamentali saranno gestite ed aggiornate dal Responsabile/Delegato Privacy Aziendale, coadiuvato dalle eventuali altre professionalità necessarie presenti in Azienda e/o di Consulenza esterna quali, ad esempio, il Responsabile dell'Ufficio Legale, il Responsabile Risorse Umane, il Responsabile IT, etc..

7.3 Regolamenti e Disciplinari - Informatici

Un'Azienda dotata di un Sistema Informativo non può essere sprovvista di alcun Regolamento e/o Disciplinare che regolamenti l'uso degli strumenti informatici e/o delle tecnologie di comunicazione oggi a disposizione.

L'illecito utilizzo della strumentazione informatica aziendale da parte dei dipendenti, può generare in capo all'azienda, una serie di responsabilità sia penali che civili, qualora non dimostri di aver adoperato tutte le precauzioni al fine di evitare il compimento delle stesse. Il principio giurisprudenziale sul quale si basa

questa necessità è il seguente: “non impedire un evento che si ha l’obbligo di impedire, equivale a cagionarlo”. Ovvero: non attivarsi al fine di impedire l’evento illecito posto in essere dal proprio dipendente, equivale a cagionare l’illecito stesso.

Uno “strumento” per cautelarsi può essere rappresentato dal Regolamento o Disciplinare informatico interno, ovvero da un documento redatto secondo la struttura e le esigenze aziendali, in cui siano contenute le specifiche relativamente all’utilizzo della strumentazione elettronica ed informatica a disposizione: dalla regolamentazione dell’installazione del software, a quella relativa all’uso della casella di posta elettronica all’utilizzo di Tablet e Smartphone. Il regolamento in parola può pertanto definirsi come quello strumento di prevenzione in grado innanzi tutto di dimostrare l’attenzione e la volontà di evitare eventi estranei all’attività lavorativa da parte dell’azienda, e dall’altra come strumento di indicazione per i dipendenti su come utilizzare le risorse informatiche aziendali senza per questo incorrere, anche in buona fede, in illeciti.

Qui di seguito si riportano i Regolamenti e i Disciplinari allegati al presente Manuale:

Codice	Tipo di documento	Descrizione
DIA	Regolamento	DIA – Disciplinare Informatico Aziendale

In merito alla Gestione della Posta Elettronica Aziendale e del Fiduciario per l’accesso alle medesime in caso d’assenza prolungata del titolare della casella, si riporta la seguente documentazione:

Codice	Tipo di documento	Descrizione
LNF	Lettera di nomina	LNF – Modello Nomina Fiduciario
VCPE	Verbale	VCPE – Verbale di comunicazione Posta Elettronica

Tali Procedure saranno gestite ed aggiornate dal Delegato Privacy Aziendale, coadiuvato dalle eventuali altre professionalità necessarie presenti in Azienda e/o di Consulenza esterna quali, ad esempio, il Consulente Privacy, il Responsabile IT, etc..

7.4 Procedura di gestione Data Breach

La presente procedura si prefigge di dettare regole di comportamento per coloro che possono essere coinvolti in fenomeni di violazione dei dati (Data Breach) e nelle necessarie e conseguenti valutazioni. In particolare, la presente procedura mira a dare chiare e semplici istruzioni ai fini d’adempiere in modo consapevole, mantenendone debito riscontro, a quanto previsto dai considerando 83, 85, 87, 88 e dagli artt. 33 e 24 GDPR 2016/679. In merito si riporta la seguente documentazione:

Codice	Tipo di documento	Descrizione
PDB	Procedura	Procedura Data Breach ver. 1.0 rev. 0
ReDaBr	Allegato 1	Registro Data Breach
DaBrVI	Allegato 2	Data Breach - Verbale di incidente di sicurezza
DaBrV	Allegato 3	Data Breach - Verbale interno Data Breach
DaBrCGC	Allegato 4	Data Breach - Comunicazione Completa al Garante
DaBrCGB	Allegato 5	Data Breach - Comunicazione Breve al Garante

Tale Procedura sarà gestite ed aggiornate dal Responsabile/Delegato Privacy Aziendale, coadiuvato dal Responsabile IT.

7.5 Procedura Valutazione Responsabili Esterni

Scopo della presente procedura è quello di procedere alla corretta valutazione dei Responsabili Esterni per il trattamento dei dati, sulla base di quanto disposto dall'art. 28 del GDPR 2016/679 e dalla normativa nazionale vigente.
La procedura di valutazione mira a determinare se il Responsabile svolge i trattamenti di propria competenza, ad esso delegati dalla L'OFFICINA DELL'AIAS Coop. Soc., nel pieno rispetto dell'attuale normativa Privacy, sia Nazionale che Europea.

Annualmente, in sede d'aggiornamento del Documento Riepilogativo del Sistema Privacy e/o della Valutazione Fornitori del Sistema Qualità, il Responsabile Privacy, coadiuvato anche da Consulenti esterni, procede alla valutazione dei Responsabili Esterni. In merito si riporta la seguente documentazione:

Codice	Tipo di documento	Descrizione
PVRST	Procedura	Procedura di valutazione Responsabile Esterno
PVRST-LTQR	Lettera	Lettera trasmissione Quest. di autovalutazione
PVRST-ADR	Allegato 1	AUTODICHIARAZIONE RESPONSABILE
QVR	Allegato 2	Questionario valutazione Responsabile

Tali norme comportamentali saranno gestite ed aggiornate dal Delegato al trattamento, coadiuvato dalle eventuali altre professionalità necessarie presenti in Azienda e/o di Consulenza esterna quali, ad esempio, il Responsabile dell'Ufficio Legale, il Responsabile Qualità, il Responsabile IT, etc..

7.6 Procedura Risposta Unica

Scopo della presente procedura è quello di adottare una procedura unica di gestione degli Atti di Designazione a Responsabile ex art. 28 GDPR 2016/679, senza dover valutare di volta in volta le singole proposte di sottoscrizione (lettere di nomina, atti di designazione o contratti), a volte stese anche in modo estremamente complesso o, peggio, in modo pressapochistico e per nulla aderente alla realtà dell'azienda. O costringendo quest'ultima a perdere diverse ore di valutazione per analizzare nel dettaglio i testi o a personalizzarli, trattandosi di moduli generici non compilati.

Inoltre, la L'OFFICINA DELL'AIAS Coop. Soc. in qualità di Responsabile, è tenuta a fornire, periodicamente (almeno annualmente), ai propri Committenti, Titolari del trattamento dei dati personali affidati, informazioni (spesso esaurienti) relative agli adempimenti Privacy e di Sicurezza adottati dall'Azienda. Tali informazioni sono essenziali per consentire al Committente di poter procedere, positivamente, alla corretta valutazione di L'OFFICINA DELL'AIAS Coop. Soc. quale Responsabile Esterno del trattamento dei dati, sulla base di quanto disposto dall'art. 32 let. d) GDPR 2016/679.
In merito si riporta la seguente documentazione:

Codice	Tipo di documento	Descrizione
PRRU	Procedura	Procedura di Risposta
LAR	Lettera	Lettera accompagnatoria Addendum Privacy Responsabile
eMAR	eMail	eMail Addendum Privacy Designazione Responsabile
DRE	Addendum Privacy	Addendum Privacy -Tipo a Responsabile Esterno - STD
DRE	Addendum Privacy	Addendum Privacy -Tipo a Responsabile Esterno - AD
DAGG	Modello	DAGG - Dichiarazione di avvenuta adozione delle misure di sicurezza

	Modello	Comunicazione Elenco Sub-Responsabili
	Informativa	Informativa Servizi in outsorcing saas e onpremise
	Modello	Documento descrittivo Infrastruttura informatica interna
	Modello	Documento descrittivo Infrastruttura informatica in Cloud

Tali Procedure saranno gestite ed aggiornate dal Delegato Privacy Aziendale, coadiuvato dalle eventuali altre professionalità necessarie presenti in Azienda e/o di Consulenza esterna quali, ad esempio, il Consulente Privacy, il Responsabile IT, etc..

7.7 Procedure e Disciplinari aziendali

In questa sezione vengono riportati strumenti e procedure necessarie a regolamentare gli accessi in azienda e/o eventuali Visite Ispettive da parte di terzi. In merito si riporta la seguente documentazione:

Codice	Tipo di documento	Descrizione
LAUR	Modello	Lettera accesso agli Uffici - RECEPTIONIST
PRIS-VI	Regolamento	Regolamento Visite Ispettive ex art. 32 let.d
RIT	Regolamento	Regolamento per l'ingresso di terzi in azienda
		Pass Visitatori - Badge tipo
ReAL-1		Registro Accesso Locali

Tali norme comportamentali saranno gestite ed aggiornate dal Delegato al trattamento, coadiuvato dalle eventuali altre professionalità necessarie presenti in Azienda e/o di Consulenza esterna quali, ad esempio, il Responsabile dell'Ufficio Legale, il Responsabile Qualità, il Responsabile IT, etc..

7.8 Istruzioni operative (Vademecum generale adempimenti Privacy)

7.8.1 Lettere d'incarico per il trattamento dei dati

a. **Titolare e Delegato**: Deve firmare il verbale annuale di redazione/revisione del DRSP e tutte le parti del manuale medesimo ad esso riservate. Le singole lettere d'incarico (RST e RDT) sono da far sottoscrivere alle persone indicate come Delegato/i Privacy e del trattamento dei dati, consegnandogli, al contempo, una copia delle stesse. L'originale firmato è da conservare nella cartella "Privacy".
b. **Incaricati**: le lettere d'incarico (IDT2 e IDT2GR) sono da far sottoscrivere alle persone indicate come Incaricati del trattamento dei dati, consegnandogli, al contempo, una copia delle stesse e, se i dati sono trattati con elaboratori elettronici, anche una copia del "Disciplinare Informatico Aziendale (DIA)". La consegna va fatta da parte del Delegato al trattamento il quale istruisce, contestualmente, l'incaricato sugli adempimenti che l'attendono (quelli scritti sulla stessa "Lettera d'incarico"). Eventualmente, il Delegato, può consegnare anche quanto disposto in materia di protezione dei dati personali ovvero copia dei modelli DTEC_O, DTEC_P e DTEC_Q. L'originale della lettera d'incarico firmato è da conservare nella cartella "Privacy".
c. **Dipendenti**: se non già fatto al momento dell'assunzione è da far sottoscrivere, consegnandone copia, il "Consenso Informato Dipendenti" (LCD). L'originale firmato è da conservare nella documentazione relativa al Personale. L'originale firmato è da conservare nella documentazione relativa al Personale.
d. **Responsabili esterni del trattamento**: Gli Addendum Privacy (DTEC_W_W2) sono da far sottoscrivere alle persone indicate come Responsabili ai trattamento, consegnandogli, al contempo, una copia delle stesse. I Responsabili ai trattamento dovranno consegnare

periodicamente, all'Azienda, anche un'autocertificazione d'adeguamento al GDPR (eventualmente può essere utilizzato il modulo predisposto e disponibile nella cartella "8.3 Documenti di uso comune \ DAGG - Dichiarazione di avvenuta adozione delle misure di sicurezza" nel CD allegato al DRSP). Gli Addendum Privacy possono essere anche spedite via raccomandata A.R. oppure via PEC ai singoli Responsabili (solo con tali mezzi la nomina avrà operatività e validità legale anche senza il riscontro scritto del Responsabile medesimo). Gli originali firmati sono da conservare nella cartella "Privacy".

e. **Amministratori di sistema**: le lettere d'incarico sono da far sottoscrivere alle persone indicate come Amministratori di Sistema Interni, Tecnici Incaricati e/o Responsabili Esterni del trattamento di dati informatici, consegnandogli, al contempo, una copia delle stesse. Le lettere possono essere anche spedite via raccomandata A.R. oppure via PEC ai singoli Responsabili Esterni (solo con tali mezzi la nomina avrà operatività e validità legale anche senza il riscontro scritto del Responsabile medesimo).

ATT.: Conviene cogliere l'occasione della consegna e firma della documentazione di cui sopra, per predisporre il sistema di autenticazione e consegnare le password di primo ingresso e il modulo e le buste per l'automodifica delle credenziali (v. Cap. 3 p. 3.1 e 3.2). Inoltre è opportuno pianificare, in tale occasione, almeno un incontro di formazione in materia di trattamento dei dati personali (Privacy) del personale incaricato.

7.8.2 Documentazione di massima da consegnare al personale dipendente

Codice Documento	Tipologia	Descrizione
IDT2	Lettera di incarico	Incaricato del trattamento dei dati personali *(Obbligatoria)*
LCD	Allegati 6.2	Consenso Informato Dipendenti *(Obbligatorio)*
DIA	Regolamento	Disciplinare Informatico Aziendale *(Obbligatorio)*
ADSCD	ADS	ADS - Comunicazione Dipendenti *(Obbligatoria)*
RAL_LCC	Doc. uso comune	Lettera consegna chiavi *(Facoltativa)*
LCEMAIL	Doc. uso comune	Lettera Consegna Credenziali EMail aziendale *(Facoltativa)*
LCP	Doc. uso comune	Lettera Consegna Strumenti Elettronici *(Facoltativa)*
LCPW	Doc. uso comune	Lettera Consegna Credenziali *(Facoltativa)*
NOCI	Istruzioni	Norme comportamentali per incaricati *(Obbligatorio)*

Annualmente di dovrà procedere all'attività di verifica dei Responsabili Esterni. La procedura in parola prevede:

a. **Responsabili Esterni del trattamento dei dati**: è necessario, come previsto dall'art. 32 le. d) GDPR 2016/679 operare una verifica valutativa dei singoli Responsabili Esterni. A tal fine è necessario richiedere ad ogni singolo Responsabile Esterno almeno una autodichiarazione d'essere "a norma" con gli adempimenti Privacy su modello del documento "*DAGG - Dichiarazione di avvenuta adozione delle misure di sicurezza*" che si trova nella seguente cartella del CD alleato al DRSP: "8.3 Documenti di uso comune". La procedura di valutazione annuale si conclude, in ogni caso, con la redazione e sottoscrizione di un apposito verbale.
b. **Amministratori di sistema**: come previsto dal Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008 si deve operare annualmente una verifica valutativa dei singoli ADS e Responsabili Esterni del trattamento di dati informatici. A tal fine è bene richiedere ad ogni singolo ADS/Responsabile Esterno almeno una autodichiarazione d'essere "a norma" con gli adempimenti Privacy come descritta al punto precedente. La procedura di valutazione annuale si conclude, in ogni caso, con la redazione e sottoscrizione di un apposito verbale.

7.8.3 Informative/Consenso informato per il trattamento dei dati

1. **(Solo a fini amministrativo-contabili) Informativa Clienti**: da consegnare a tutti i Clienti di cui si trattano i dati personali. Consegnare una copia (meglio se spedita via eMail/fax conservandone copia almeno elettronica).
2. **(A fini amministrativo-contabili, commerciali, altre finalità necessitanti specifico consenso) Consenso Informato Clienti/Pazienti/Utenti** (è in alternativa al punto precedente): da consegnare a tutti i Clienti/Pazienti/Utenti di cui si trattano i dati personali. Consegnare una copia e conservare l'originale firmato nella cartella "Privacy". Il Consenso può essere spedito via eMail/fax, conservandone copia almeno elettronica sia della spedizione che di quanto ricevuto.
3. **(Solo a fini amministrativo-contabili) Informativa Fornitori**: da consegnare a tutti i Fornitori di cui si trattano i dati personali. Consegnare una copia e conservare l'originale firmato nella cartella "Privacy" (meglio se spedita via eMail/fax conservandone copia almeno elettronica).
4. Predisporre un elenco dei Clienti / Pazienti / Utenti / Fornitori recante quali sono stati contattati con la consegna delle Informative e dei consensi di cui ai punti 1, 2 e 3 da conservare nella cartella "Privacy".
5. **Informativa dipendenti**: da consegnare e far firmare a tutti i dipendenti e collaboratori, consegnarne una copia e conservare l'originale firmato nella documentazione relativa al Personale. Contestualmente conviene, in caso di trattamento dei dati con elaboratori elettronici e, se non già consegnato, dare anche una copia del "Disciplinare Informatico Aziendale (DIA)".
6. **Se l'Azienda/Studio tratta dati sensibili/sanitari: Consenso Informato Pazienti:** da consegnare a tutti i Pazienti di cui si trattano i dati personali. Consegnare una copia e conservare l'originale firmato nella cartella "Privacy".
    a. Ai punti 1, 2 e 3 si può ovviare, **per la sola parte informativa ma non per la parte consensuale**, mediante l'indicazione di una "informativa breve" (reperibile nel documento "*CLDIV Clausole Privacy Diverse*" che si trova nella seguente cartella del CD alleato al DRSP: "8.3 Documenti di uso comune") sulla diversa documentazione Aziendale/di Studio (Fatture, DDT, Preventivi, Carta intestata, etc.) che rimandi esplicitamente, mediante l'indicazione di un link, alle informative pubblicate sul sito internet dell'Azienda/Studio, come riportato nel documento "*Note di uso materiale per sito web*" che si trova nella seguente cartella del CD alleato al DRSP: "8.3 Documenti di uso comune\8.3.2 Privacy Sito Web"

7.8.4 Misure di Sicurezza – Documentazione Cartacea

a. **Regolamentazione accessi ai dati/conservazione della documentazione cartacea**:
    i. Predisporre un apposito registro per l'accesso ai locali contenenti dati personali (ad es. all'Archivio) al di fuori degli orari di lavoro.
    ii. Se prevista una apposita procedura di regolamentazione e controllo degli accessi e degli appositi registri/badge si deve far riferimento a quanto riportato nel DRSP alla scheda "*DTEC_O - Modalità di protezione dei dati e dei locali*" e alla documentazione da essa richiamata.
    iii. I dati sensibili e giudiziari devono essere conservati in armadi/cassettiere dotate di chiusura a chiave (anche tutta la documentazione relativa al Personale).
    iv. Tutti i locali contenenti dati devono avere porte con serratura e, se possibile, un cartello con chiaramente indicato che l'accesso è consentito solo al personale autorizzato (v. p. vii).
    v. I faldoni/raccoglitori/cartelle d'archivio, usati per la catalogazione della documentazione contenente dati, non devono avere richiami anagrafici di terzi sui dorsi a vista.
    vi. La documentazione, oggetto temporaneo di trattamento, è bene sia conservata in cartelline.
    vii. Predisporre dei cartelli recanti la scritta "Accesso al solo personale autorizzato" da apporre alle porte/ingressi delle stanze contenenti dati personali di terzi e non riservate a ricevere il pubblico e/o altri soggetti.
b. **Antincendio:** sarebbe opportuno che i locali siano a norma con la vigente legge per l'antincendio (estintori).
c. **Distruggi-documenti**: Nei locali amministrativi dev'essere presente un sistema "distruggi-documenti" per la distruzione fisica dei documenti recanti dati personali in caso di loro eliminazione per qualsiasi motivo.

d. **Archivio**: l'archivio storico della documentazione aziendale contenente dai personali dev'essere riposto in un locale con chiusura a chiave e predisposto specificatamente un registro d'accesso, da compilarsi qualora vi si acceda oltre gli orari stabiliti di lavoro. Tutti i dati sensibili e giudiziari devono essere contenuti in armadi con chiusura a chiave (dovrà esservi almeno un armadio/cassettiera con chiusura a chiave per la documentazione relativa al personale).

7.8.5 Misure di Sicurezza – Trattamento con ELABORATORI ELETTRONICI

a. **Antivirus**: tutte le macchine devono essere dotate di software antivirus (obbligatoriamente se basate su Microsoft Windows e/o Apple Mac OS. Facoltativo se basate su Linux e/o altri sistemi operativi), aggiornato almeno semestralmente, a prescindere che siano collegate ad internet oppure no. E' opportuno abilitare il file di registro (detto anche "file di log") che monitorizza l'attività del software (aggiornamenti ed interventi) da stampare almeno annualmente (o masterizzare) e da conservare nella cartella "Privacy".
b. **Sistema anti intrusione (Firewall)**: nel caso le macchine (anche una sola) siano collegate ad internet è necessaria la presenza di un Firewall (hardware o software che sia). E' opportuno abilitare il file di registro (detto anche "file di log") che monitorizza l'attività del software/hardware (aggiornamenti ed interventi) da stampare almeno annualmente (o masterizzare) e da conservare nella cartella "Privacy".
c. **Sistema di backup**: tutti i file contenenti dati devono essere sottoposti a copia di sicurezza (backup), siano essi legati al software gestionale che sparsi tra le varie macchine in cartelle locali. Tale operazione dev'essere almeno settimanale. Nel caso sia automatizzabile con un software specifico è opportuno abilitare il file di registro (detto anche "file di log") che monitorizza l'attività del software/hardware (aggiornamenti ed interventi) da stampare annualmente (o masterizzare) e da conservare nella cartella "Privacy". In alternativa è da predisporre un registro sul quale annotare settimanalmente le operazioni di backup.
d. **Credenziali d'accesso**: tutte le macchine devono essere dotate di un sistema operativo tipo MS Windows 7/8/10 o Linux o MACOS X al fine di poter gestire correttamente le "credenziali d'accesso" come previsto dalla normativa. Macchine con vecchi Sistemi Operativi, ormai non più supportati dal produttore (ad es. con MS Windows 95/98/2000/XP/VISTA) non sono assolutamente a norma (sono da cambiare!). La gestione delle credenziali può essere fatta nel seguente modo:
    1. La parola chiave (**password**), dev'essere composta da **minimo 8 caratteri** e massimo 12;
    2. **Non deve contenere riferimenti agevolmente riconducibili all'incaricato**
    3. **Deve essere modificata** (il sistema DEVE essere programmato per richiedere automaticamente il cambio password, MA non è obbligo che la password nuova debba essere diversa dalla vecchia) dall'incaricato al primo utilizzo e, successivamente, almeno **ogni 6 mesi**. In caso di trattamento di **dati sensibili e di dati giudiziari** la parola chiave è modificata almeno **ogni 3 mesi.**
    4. Il codice per l'identificazione ("**user**" **o** "**nome utente**") non può essere assegnato ad altri incaricati, neppure in tempi diversi (ovvero: **1 persona 1 "nome utente"**)
    5. Le credenziali di autenticazione (**"nome utente" + password**) **non utilizzate da almeno sei mesi sono disattivate**, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
    6. **Se il sistema informatico è ben programmato e strutturato non risulta necessaria anche l'organizzazione della tracciatura cartacea dei cambi password**. L'unica busta da creare è quella con le credenziali tecniche d'accesso che consentono di poter accedere ai server/macchine che presiedono ai sistemi d'autenticazione.
e. **Protezioni hardware**: ciascuna macchina, ed in particolare l'eventuale Server, dovrà essere dotata di Gruppo di Continuità elettrica ed essere sistemata sollevata da terra.
f. **Server:** le macchine fungenti da server di rete e contenenti gli archivi dei dati personali non devono essere ad immediata disposizione di persone terze all'Azienda (ovvero non devono essere allocate liberamente in corridoi, reception, locali aperti al pubblico). In questo caso devono essere conservate in un apposito armadio con chiusura a chiave.

Si ricorda che dal 15 dicembre 2009 è in vigore quanto previsto dal Provvedimento del Garante per la Privacy del 27 novembre 2008 pubblicato in G.U. nr. 300 del 24 dicembre 2008 in merito all'attività svolta dagli Amministratori di Sistema. Oltre alla parte documentale è necessario:

PORRE IN ESSERE UN SISTEMA DI REGISTRAZIONE E CONSERVAZIONE DEI FILE DI LOG (Registri) DEI SERVER/PC CONTENENTI DATI PERSONALI

SE **AZIENDA NON STRUTTURATA** o DATI NON PARTICOLARMENTE SENSIBILI/GIUDIZIARI:

1. **RACCOLTA LOG:** abilitare nei server/PC la creazione automatica dei file di log (ad es. in MS Windows: Log Eventi Protezione/Security) con una durata/dimensione **CONGRUA** a consentire l'operazione di conservazione semestrale.
2. **ESPORTAZIONE/COPIA** dei file di log in formato opportuno.
3. **MASTERIZZAZIONE** dei file di log almeno mensile su CD e conservazione dello stesso almeno semestrale.

SE **AZIENDA STRUTTURATA** o DATI PARTICOLARMENTE SENSIBILI/GIUDIZIARI:

1. **DOTARSI DI UN SOFTWARE CHE CONSENTA L'ARCHIVIAZIONE DEI LOG IN TEMPO PRESSOCHÉ' REALE**.
2. **MASTERIZZAZIONE** dei file di log almeno mensile su CD e conservazione dello stesso almeno semestrale.

8 Allegati

LEGENDA delle Figure Privacy

TIPO	DESCRIZIONE
T	Titolare del trattamento dei dati
RDT	Delegato Privacy
RSTN	Delegato al trattamento dei dati con potere di nomina
RST	Delegato al trattamento dei dati senza potere di nomina
IDT	Incaricato
ADSI	Amministratore di Sistema Interno
ADST	Amministratore di Sistema Tecnico Incaricato
BKP	Incaricato del backup
CDP	Incaricato della custodia delle password

CONSERVAZIONE DEI DOCUMENTI PRIVACY: Tutta la documentazione Privacy va conservata nella propria specifica cartella, generalmente negli uffici del Titolare del Trattamento e/o del Delegato al trattamento, tranne per quei documenti ove è prescritto un luogo specificatamente diverso.

8.0 Gestione e tempi di conservazione della modulistica allegata (7.0)

8.0.1 Formazione (7.1)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
	Manuale	Manuale per l'utente - pillole di privacy	RDT, Consulente Privacy		10 anni RDT	02.07.17	28.12.18			
	Manuale	Manuale per Titolare e Delegati	RDT, Consulente Privacy		10 anni RDT	02.07.17	28.12.18			
DIA	Disciplinare	Disciplinare Informatico Aziendale	RDT, ADS, Consulente Privacy		10 anni RDT	02.07.17	28.12.18			
	Manuale	ADS - Amministratori di Sistema - Note e Procedura di Trattamento	Legislatore, Garante		10 anni RDT	02.07.17	28.12.18			
	Slide	Slide corso di formazione generale sulla Privacy	Consulente Privacy		10 anni RDT	02.07.17	28.12.18			
	Normativa	Regolamento Europeo GDPR 2016/679	Legislatore, Garante		10 anni RDT	02.07.17	28.12.18			
	Normativa	Testo unico sul trattamento dei dati - Dlgs 196-03	Legislatore, Garante		10 anni RDT	02.07.17	28.12.18			

8.0.2 Istruzioni Incaricati (7.2)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
NOCI	Istruzioni	Norme comportamentali - Incaricati	RDT, Consulente Privacy		10 anni RDT	02.07.17	28.12.18			

NOCD	Istruzioni	Norme comportamentali - Delegati	RDT, Consulente Privacy		10 anni RDT	02.07.17	28.12.18			

8.0.3 Disciplinari e Regolamenti Informatici (7.3)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
DIA	Regolamento	Disciplinare informatico aziendale	T, RDT, ADSI		10 anni RDT	02.07.17	28.12.18			
RTS	Regolamento	Regolamento per l'uso di Tablet e Smartphone	T, RDT, ADSI		10 anni RDT	02.07.17	28.12.18			
RPN	Regolamento	Politiche di Network Access Control (NAC)	T, RDT, ADSI		10 anni RDT	02.07.17	28.12.18			
		Lettera di nomina Fiduciario Posta Elettronica ISTRUZIONI	RDT, ADSI	ADSI, ADST, T, RSTN, RST, IDT	10 anni RDT	02.07.17	28.12.18			
LNF	Nomina	Lettera di nomina Fiduciario Posta Elettronica	RDT, ADSI	ADSI, ADST, T, RSTN, RST, IDT	10 anni RDT	02.07.17	28.12.18			
VCPE	Modello	Verbale di comunicazione Posta Elettronica	RDT, ADSI	ADSI, ADST, T, RSTN, RST, IDT	10 anni RDT	02.07.17	28.12.18			

8.0.4 Procedura Data Breach (7.4)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
PDB	Procedura	Procedura di gestione Data Breach	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			
ReDaBr	Registro	Registro Data Breach	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DaBrVI	Verbale	Data Breach - Verbale di incidente di sicurezza	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DaBrV	Verbale	Data Breach - Verbale interno Data Breach	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DaBrCGC	Verbale	Data Breach - Comunicazione Completa al Garante	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DaBrCGB	Verbale	Data Breach - Comunicazione Breve al Garante	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			

8.0.5 Valutazione Responsabili Esterni (7.5)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
PVRST	Procedura	Procedura di valutazione Responsabile Esterno	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			
PVRST-ADR	Modello	AUTODICHIARAZIONE RESPONSABILE	T, RDT	Responsabile	10 anni RDT	02.07.17	28.12.18			
PVRST-QVR	Modello	Questionario di autovalutazione Responsabile Esterno	T, RDT	Responsabile	10 anni RDT	02.07.17	28.12.18			
PVRST-LTQR	Modello	Lettera trasmissione Quest. di autovalutazione	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			

PVRST-VA	Verbale	Verbale di verifica annuale Responsabili Esterni	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			
ADSVE - ADS	Verbale	Verbale di verifica annuale	T, RDT, ADSI	RDT, ADSI	10 anni RDT	02.07.17	28.12.18			

8.0.6 Procedura di Risposta Unica (7.6)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
PRRU	Procedura	Procedura di Risposta	T, RDT		10 anni RDT	02.07.17	28.12.18			
LAR	Lettera	Lettera accompagnatoria Addendum Privacy Responsabile	T, RDT	Responsabile	10 anni RDT	02.07.17	28.12.18			
eMAR	eMail	eMail accompagnatoria Addendum Privacy Responsabile	T, RDT	Responsabile	10 anni RDT	02.07.17	28.12.18			
DRE	Addendum Privacy	Addendum Privacy-Tipo a Responsabile Esterno - STD	T, RDT	Responsabile	10 anni RDT	02.07.17	28.12.18			
DRE	Addendum Privacy	Addendum Privacy-Tipo a Responsabile Esterno - AD	T, RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DAGG	Modello	DAGG - Dichiarazione di avvenuta adozione delle misure di sicurezza	T, RDT, Resp. Area, Resp. IT	RDT, Resp. Area, Resp. IT	10 anni RDT	02.07.17	28.12.18			
	Modello	Comunicazione Elenco Sub-Responsabili	T, RDT, Resp. Area, Resp. IT	RDT, Resp. Area, Resp. IT	10 anni RDT	02.07.17	28.12.18			
	Informativa	Informativa Servizi in outsorcing saas e onpremise	T, RDT, Resp. Area, Resp. IT	RDT, Resp. Area, Resp. IT	10 anni RDT	02.07.17	28.12.18			

8.0.7 Procedure e Disciplinari Aziendali (7.7)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
PRIS-VI	Regolamento	PRIS-VI - Regolamento Visite Ispettive	T, RDT		10 anni RDT	02.07.17	28.12.18			
LAUR	Lettera	LAUR - Lettera accesso agli Uffici - RECEPTIONIST	T, RDT		10 anni RDT	02.07.17	28.12.18			
RIT	Regolamento	RIT - Regolamento per l'ingresso di terzi in azienda	T, RDT		10 anni RDT	02.07.17	28.12.18			
ReAL-1	Registro	ReAL-1 Registro Accesso Locali	T, RDT		10 anni RDT	02.07.17	28.12.18			
	Modello	Pass visitatore	T, RDT		10 anni RDT	02.07.17	28.12.18			

8.0.8 Vademecum (7.8)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
DPSIO	Vademecum	Istruzioni operative base	T, RDT, ADSI		10 anni RDT	02.07.17	28.12.18			
	Promemoria	Promemoria Privacy base	T, RDT, ADSI		10 anni RDT	02.07.17	28.12.18			

8.1 Elenco dei modelli allegati (Modelli e Lettere d'Incarico)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
MANUALE	Manuale	Manuale D.R.S.P.	T, RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
RDT	Nomina	Delegato Privacy	T, RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
RST	Nomina	Delegato interno al trattamento dei dati	T, RDT	T, RSTN, RST	10 anni RDT	02.07.17	28.12.18			
IDT2	Nomina	Incaricato del trattamento dei dati personali	T, RDT	RSTN, IDT	10 anni RDT	02.07.17	28.12.18			
IDT2GR	Nomina	Incaricato del trattamento dei dati personali, per unità organizzativa e/o mansione omogenea	T, RDT	RSTN, IDT	10 anni RDT	02.07.17	28.12.18			
GMSE	Nomina	Incaricato gestione e manutenzione strumenti elettronici	T, RDT	T, RDT, IDT	10 anni RDT	02.07.17	28.12.18			
CDP	Nomina	Incaricato della custodia delle copie delle credenziali	T, RDT	T, RDT, IDT	10 anni RDT	02.07.17	28.12.18			
BKP	Nomina	Incaricato delle copie di sicurezza	T, RDT	T, RDT, IDT	10 anni RDT	02.07.17	28.12.18			
RAL_LCC	Lettera di consegna	Controllo degli accessi alle aree ai locali e consegna chiavi	T, RDT	RDT, RESP. RISORSE UMANE, IDT	10 anni RDT	02.07.17	28.12.18			
LAUR	Lettera di consegna	Lettera accesso agli Uffici	T, RDT	RDT, RESP. RISORSE UMANE, IDT	10 anni RDT	02.07.17	28.12.18			
DTEC_W_W2	Addendum Privacy	Responsabile esterno al trattamento dei dati ex art. 28 GDPR 2016/679	T, RDT	T, RST EST.	10 anni RDT	02.07.17	28.12.18			
DTEC_A	Modello	Elenco degli archivi dei dati oggetto del trattamento	RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DTEC_B	Modello	Elenco delle sedi/uffici in cui vengono trattati i dati	RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DTEC_C	Modello	Scheda riepilogativa del Sistema informativo aziendale	RDT	RDT, ADSI	10 anni RDT	02.07.17	28.12.18			
DTEC_D	Modello	Sistemi di elaborazione per il trattamento dei dati	RDT	RDT, ADSI	10 anni RDT	02.07.17	28.12.18			
DTEC_E	Modello	Enti terzi a cui è affidato il trattamento dei dati in out-sourcing	RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DTEC_F	Modello	Personale autorizzato al trattamento dei dati	RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
DTEC_J	Modello	Distribuzione dei compiti e delle responsabilità	RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
DTEC_G	Modello	Permessi di accesso ai dati	RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
DTEC_H_N	Modello	Piano di formazione del personale autorizzato al trattamento dei dati	RDT	RDT	10 anni RDT	02.07.17	28.12.18			
DTEC_M	Prescrizione	Criteri e procedure per garantire l'integrità dei dati informatici	T, RDT		10 anni RDT	02.07.17	28.12.18			
DTEC_O	Prescrizione	Modalità di protezione dei dati e dei locali	T, RDT		10 anni RDT	02.07.17	28.12.18			
DTEC_P	Prescrizione	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari	T, RDT		10 anni RDT	02.07.17	28.12.18			
DTEC_Q	Prescrizione	Modalità di trattamento senza l'ausilio di strumenti elettronici	T, RDT		10 anni RDT	02.07.17	28.12.18			
DTEC_S	Modello	Criteri di assegnazione password nei sistemi di elaborazione	T, RDT		10 anni RDT	02.07.17	28.12.18			

DTEC_Z-1	Modello	Valutazione rischi sul trattamento dei dati – TABELLA DESCRITTIVA	T, RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
DTEC_Z-2	Modello	Valutazione rischi sul trattamento dei dati – TABELLA OPERATIVA	T, RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			

8.2 Amministratori di Sistema (ADS)

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
ADSVN	Verbale	Verbale annuale di nomina o verifica ADS	T, RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
ADSEL	Modello	Elenco degli ADS	T, RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
ADSCD	Modello	Comunicazione Dipendenti	T, RDT		10 anni RDT	02.07.17	28.12.18			
ADSIN	Nomina	Lettera di nomina ADS Interno	RDT	T	10 anni RDT	02.07.17	28.12.18			
ADSRE	Addendum Privacy	Addendum Privacy Responsabile Esterno nel trattamento di dati informatici	RDT	T	10 anni RDT	02.07.17	28.12.18			
ADSRN	Lettera	Richiesta nominativi	RDT	T, RDT	10 anni RDT	02.07.17	28.12.18			
ADSIDT2	Nomina	Lettera Incarico Trattamento - Stagista Tecnico	RDT	T, RDT, ADSI	10 anni RDT	02.07.17	28.12.18			
ADSIN2	Nomina	Lettera Incarico ADS Tecnico incaricato interno	RDT	T	10 anni RDT	02.07.17	28.12.18			

8.2.1 Normativa

ALLEGATO	DESCRIZIONE
X	**Provvedimento del Garante del 27 novembre 2008**
X	**Provvedimento del Garante del 12 febbraio 2009**
X	**Provvedimento del Garante del 21 aprile 2009**
X	**Provvedimento del Garante del 25 giugno 2009**
X	**Precisazioni del Garante del 10 dicembre 2009**

8.3 Documenti di uso comune

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
CDR	Lettera	Clausola di Confidential Agreement	RDT	RDT	10 anni RDT	02.07.17	28.12.18			
CLDIV	Modello	Clausole diverse Privacy	RDT	RDT	10 anni RDT	02.07.17	28.12.18			
CTX	Modello	Copertina telefax - Tipo	RDT	Chiunque	10 anni RDT	02.07.17	28.12.18			
DAGG	Modello	Dichiarazione di avvenuta adozione delle misure di sicurezza	RDT	RDT	10 anni RDT	02.07.17	28.12.18			
LCC	Lettera	Lettera Consegna Chiavi di accesso agli Uffici	RDT	RDT, RESP. RISORSE UMANE	10 anni RDT	02.07.17	28.12.18			

LCEMAIL	Lettera	Mail - Lettera Consegna Credenziali EMail aziendale	RDT, ADSI	Chiunque abbia una eMail az.le	10 anni RDT	02.07.17	28.12.18			
LCP	Lettera	Lettera Consegna Strumenti Elettronici	RDT, ADSI	Chiunque abbia uno Str.Elett. az.le	10 anni RDT	02.07.17	28.12.18			
LCPW	Lettera	Lettera Consegna Credenziali	RDT, ADSI	Chiunque abbia un accesso dall'esterno ai sw az.li	10 anni RDT	02.07.17	28.12.18			
MFE	Modello	Firma eMail	RDT		10 anni RDT	02.07.17	28.12.18			
MRDF	Modello	Modulo raccolta contatti fieristici	RDT	CLIENTI, UTENTI, PROSPECT	10 anni RDT	02.07.17	28.12.18			
RAL_LCC	Lettera	Controllo degli accessi alle aree ai locali e consegna chiavi	RDT	RDT, RESP. RISORSE UMANE	10 anni RDT	02.07.17	28.12.18			

8.3.1 Informative e Consensi

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
LCD	Informativa	Informativa – Collaboratori e Dipendenti	RDT	PERSONALE	10 anni RDT	02.07.17	28.12.18			
LCR	Consenso	LCR Informativa E-recruitment	RDT	PERSONALE	10 anni RDT	02.07.17	28.12.18			
LCP	Consenso	LCP Consenso informato pazienti - OSPITI	RDT	PERSONALE	10 anni RDT	02.07.17	28.12.18			
LCR	Consenso	LCR Informativa E-RECRUITMENT	RDT	PERSONALE	10 anni RDT	02.07.17	28.12.18			
LCT	Consenso	LCT Consenso informato - INTERINALI	RDT	PERSONALE	10 anni RDT	02.07.17	28.12.18			
LIE-CL	Informativa	Informativa – Clienti	RDT	CLIENTI	10 anni RDT	02.07.17	28.12.18			
LCE	Consenso	Consenso informato - Clienti	RDT	CLIENTI, UTENTI	10 anni RDT	02.07.17	28.12.18			
LIE-FR	Informativa	Informativa – Fornitori	RDT	FORNITORII	10 anni RDT	02.07.17	28.12.18			

8.3.2 Privacy Sito Web

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
DTEC_U	Modello	Valutazione sito internet	RDT	RDT	10 anni RDT	02.07.17	28.12.18			
	Istruzioni	Note di uso materiale per sito web	RDT		10 anni RDT	02.07.17	28.12.18			
	Istruzioni	Nuova Cookies law	RDT		10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet - Info legali e Clausola copyright	RDT		10 anni RDT	02.07.17	28.12.18			
	Informativa	Area Internet - Informativa sito web	RDT		10 anni RDT	02.07.17	28.12.18			

	Informativa	Area Internet - Informativa Cookie	RDT		10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet - Clausola Form Contatti	RDT	CLIENTI, UTENTI	10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet – Job Opportunities	RDT	CLIENTI, UTENTI	10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet - Newsletter	RDT	ADSI, ADST, AREA COMM.	10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet - DEM	RDT	ADSI, ADST, AREA COMM.	10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet - Clausola Form Registrami	RDT	CLIENTI, UTENTI	10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet - Clausola Form Registrazione APP	RDT	CLIENTI, UTENTI	10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet – Clausula Form Download	RDT	ADSI, ADST	10 anni RDT	02.07.17	28.12.18			
	Modello	Area Internet - Clausola Form Support Online	RDT	ADSI, ADST	10 anni RDT	02.07.17	28.12.18			

8.4 Allegati - Registri

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
ReAL-1	Registro	Registro Accesso Locali	RDT	Chiuunque	10 anni RDT	02.07.17	28.12.18			
ReAL-2	Registro	Registro Accesso Locali dopo l'orario di chiusura	RDT	Chiuunque	10 anni RDT	02.07.17	28.12.18			
RRAC	Registro	Registro dei Rischi e delle Azioni Correttive	RDT	RDT, ADSI, RSTN, RST	10 anni RDT	02.07.17	28.12.18			
ReCSD	Registro	Registro Carico Scarico documenti	RDT	Chiuunque	10 anni RDT	02.07.17	28.12.18			
ReDD	Registro	Registro Distruzione documenti	RDT	Chiuunque	10 anni RDT	02.07.17	28.12.18			
ReB	Registro	Registro Backup	RDT, ADSI	ADSI, BKP, ADST	10 anni RDT	02.07.17	28.12.18			
SKRHW	Scheda	Scheda Rischio Hardware	RDT, ADSI	ADSI, ADST	10 anni RDT	02.07.17	28.12.18			
SKRSW	Scheda	Scheda Rischio Software	RDT, ADSI	ADSI, ADST	10 anni RDT	02.07.17	28.12.18			
SKRV	Scheda	Scheda Rilevazione contagio Virus	RDT, ADSI	ADSI, ADST	10 anni RDT	02.07.17	28.12.18			

8.5 Allegati - Gestione Password e Credenziali

COD.	TIPO	DESCRIZIONE	Redazione e Emissione	Compilaz.	Conservaz e Responsab.	REVISIONI				
						00	01	02	03	04
ReGP	Registro	Registro Gestione Password	RDT, ADSI	CDP	10 anni RDT	02.07.17	28.12.18			
SAI	Istruzioni	Sistema Autenticazione istruzioni custodia password	RDT, ADSI	---	10 anni RDT	02.07.17	28.12.18			
SAIN	Istruzioni	Sistema Autenticazione istruzioni custodia password - notebook	RDT, ADSI	---	10 anni RDT	02.07.17	28.12.18			

SAMP1	Modulo	Sistema Autenticazione modulo prima consegna password	RDT	ADSI, ADST, CDP, T, RSTN, RST, IDT	10 anni RDT	02.07.17	28.12.18			
SAMP	Modulo	Sistema Autenticazione modulo custodia password	RDT	T, RSTN, RST, IDT	10 anni RDT	02.07.17	28.12.18			
SAN	Istruzioni	Sistema Autenticazione note incaricato custodia pw	RDT, ADSI	---	10 anni RDT	02.07.17	28.12.18			