

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

PREMESSA

Il Documento Programmatico per la Sicurezza dei dati (di seguito DPS) è predisposto ai sensi delle disposizioni contenute nel Capo II – Misure minime di sicurezza del Titolo V – Sicurezza dei dati e dei sistemi del Codice in materia di protezione dei dati personali approvato con D. Lgs. 30 giugno 2003, n. 196.

Il DPS si propone l'obiettivo di dettare norme di sicurezza dei dati personali trattati dal Consorzio. In particolare il DPS individua i trattamenti dei dati, definisce le figure interessate dal trattamento dati, ne definisce i compiti, analizza i rischi ed individua le modalità di protezione da essi e le eventuali misure per rimediare agli eventi occorsi, pregiudizievoli della riservatezza dei dati.

CONTENUTI

1. Elenco dei trattamenti di dati personali effettuati
2. Distribuzione delle responsabilità tra le figure individuate dal Codice
3. Definizione dei compiti per ogni figura
4. Analisi dei rischi incombenti sui dati
5. Individuazione delle misure di protezione per i dati, gli elementi di custodia (arredi e attrezzature informatiche) ed i locali ove tali elementi sono ubicati, distinguendo tra trattamento con strumenti elettronici e trattamento senza strumenti elettronici
6. Descrizione dei criteri per il ripristino dei dati, a seguito di distruzione o danneggiamento
7. Previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati e delle misure disponibili per prevenire eventi dannosi
8. Descrizione dei criteri da adottare per garantire il rispetto di misure minime di sicurezza in caso di trattamenti di dati personali affidati a soggetti esterni all'amministrazione

1 ELENCO DEI TRATTAMENTI DI DATI PERSONALI EFFETTUATI

I dati trattati dal Consorzio possono essere raggruppati in tre distinte categorie:

- a) dati relativi al servizio sociale: si tratta di trattamento finalizzato alla prevenzione e rimozione del disagio socio-economico dei cittadini dei comuni consorziati, nell'ambito dell'attività istituzionale cui il C.I.S.S.A. è preposto, attraverso l'erogazione di servizi di varia natura;
- b) dati relativi alla gestione del personale e dei componenti degli organi di amministrazione e controllo (di seguito più brevemente "gestione personale"): si tratta di trattamento finalizzato alla gestione e conseguente remunerazione delle prestazioni lavorative da parte di soggetti assunti dal Consorzio mediante contratto di lavoro subordinato o a titolo di consulenza e all'esercizio delle attività di amministrazione e controllo da parte degli organi istituzionali, con la relativa remunerazione;
- c) dati relativi alla contabilità: si tratta del trattamento finalizzato all'affidamento di fornitura di beni o servizi a soggetti esterni all'amministrazione e alla loro conseguente remunerazione.

2 DISTRIBUZIONE DELLE RESPONSABILITÀ

Nell'ambito del Consorzio, le figure previste dal Codice in materia di protezione dei dati personali sono di seguito individuate:

Titolare del trattamento (art. 28 del Codice): è il C.I.S.S.A. stesso

Responsabile del trattamento (art. 29 del Codice): è il Direttore del Consorzio; in caso di sua assenza prolungata (p. es. per congedo ordinario o per malattia prolungata), il Responsabile del trattamento è temporaneamente individuato (fino al rientro del Direttore del Consorzio) nella persona del funzionario in servizio, con maggiore anzianità di servizio nel Consorzio.

Incaricati del trattamento (art. 30 del Codice): è ogni operatore del Consorzio, compresi i Responsabili di Area ed il Direttore del Consorzio – Responsabile del trattamento. Essendo tutta l'attività del Consorzio finalizzata all'erogazione di servizi sociali alla persona, si ritiene di individuare ogni dipendente come incaricato, in quanto, per l'espletamento di qualsiasi pratica, anche le più semplici, si richiede il contatto con dati personali (sensibili o comuni)

Custode delle password (p.to 10 del Disciplinare tecnico in materia di misure minime di sicurezza): è un soggetto nominato dal Responsabile del trattamento, per la custodia delle password di accesso agli elaboratori e ai diversi software operativi; accanto al custode sono previsti 2 vice custodi che svolgono le funzioni attribuite al custode in caso di sua assenza; in caso di mancanza di nomina del custode o dei vice custodi o in caso di assenza prolungata di uno di essi, il ruolo vacante è assunto (fino alla nomina o al termine dell'assenza) dal Responsabile del trattamento

Inoltre, vengono individuate le seguenti figure ulteriori:

Amministratore di sistema: è la ditta incaricata della manutenzione dell'hardware e delle reti

Responsabile del trattamento per dati trattati all'esterno: sono i soggetti cui il Consorzio trasferisce dati, raccolti presso gli interessati, indispensabili per la corretta gestione dei servizi affidati all'esterno.

3 DEFINIZIONE DEI COMPITI

Titolare

Responsabile

- nomina/revoca tutti gli incaricati, definendone eventualmente le rispettive sfere di competenza;
- nomina/revoca il custode delle password e 2 vice custodi;
- nomina/revoca l'amministratore di sistema;
- tutte le nomine/revoche devono essere fatte in forma scritta;
- individua tutte le modalità di trattamento;
- predispone annualmente, nel rispetto delle scadenze stabilite per legge o regolamento, il DPS, da sottoporre all'approvazione del Consiglio di Amministrazione;
- procede alla verifica, anche a campione, dell'osservanza delle modalità di trattamento dati e del rispetto delle misure minime di sicurezza da parte dei soggetti individuati ai sensi del Codice;
- predispone la modulistica finalizzata a tutelare il diritto di accesso ai dati personali (artt. 7 – 10 del Codice) e a fornire adeguata informazione ai soggetti presso i quali i dati sono raccolti (art. 13);
- individua procedure per la distruzione dei dati qualora eccedenti o non più utili alle finalità istituzionali dell'Ente;
- coordina, in accordo con i Responsabili di Area, l'attività formativa finalizzata ad istruire ed aggiornare gli incaricati e gli altri soggetti sui rischi e sulle precauzioni da adottare in ambito di trattamento dati e sulle innovazioni normative;

Incaricato

- esegue con professionalità i compiti specificati per iscritto dal Responsabile, all'atto di nomina.

Custode delle password (e vice custodi)

- cura con riservatezza la custodia delle password di accesso agli elaboratori e, ove presenti, ai software, adottando le misure di sicurezza successivamente specificate.

Amministratore di sistema

- gestisce l'assistenza hardware e software secondo le istruzioni impartite dal Responsabile, all'atto di nomina;
- in caso gestisca anche operazioni di back up o comunque venga in contatto con dati personali raccolti dagli incaricati del Consorzio, osserva le disposizioni previste per i Responsabili del trattamento per dati trattati all'esterno;
- gli accessi al sistema da parte dell'Amministratore di Sistema sono monitorati tramite apparecchiature hardware e software (LogStore Box) collegate direttamente ai server del Consorzio e gestiti da terzi fornitori, nel rispetto delle disposizioni del Garante assunte con provvedimento del 27 novembre 2008, modificate con provvedimento del 25 giugno 2009;

Responsabile del trattamento per dati trattati all'esterno:

- effettua il trattamento dati secondo le istruzioni impartite dal Responsabile, all'atto di nomina;
- in questo caso trovano applicazione i *Criteri per garantire misure minime di sicurezza per dati affidati all'esterno*, di seguito individuati.

4 ANALISI DEI RISCHI

I rischi individuati nell'ambito del trattamento dei dati possono essere raggruppati nelle seguenti classi:

a) distruzione o smarrimento dei dati:

- la *distruzione* dei dati ricorre quando dati necessari allo svolgimento di attività istituzionale vengono irrimediabilmente distrutti o danneggiati in misura tale da renderne impossibile il recupero nella forma e con il contenuto informativo originario;
- lo *smarrimento* dei dati ricorre quando dati necessari allo svolgimento di attività istituzionale vengono smarriti definitivamente, senza possibilità di recupero nella forma o con il contenuto informativo originario;

b) accesso non autorizzato ai dati: ricorre quando per incuria degli incaricato preposti o eludendo le misure di sicurezza, un soggetto non autorizzato (interno o esterno all'amministrazione) ha accesso a dati personali;

c) trattamento in modalità non conforme alla legge o al regolamento: ricorre quando un soggetto incaricato al trattamento dati effettua le operazioni cui è preposto in modo difforme dalla legge o dai regolamenti, per incuria, disattenzione, non perfetta conoscenza delle norme, o anche per cause di forza maggiore, senza che ciò cagioni necessariamente un danno al soggetto cui i dati si riferiscono.

Al fine di limitare i rischi precedentemente identificati, si individuano le misure di protezione dei dati da osservare da parte dei diversi soggetti preposti, a vario titolo, al trattamento dati.

In caso di evoluzione tecnologica e/o di aggiornamento dell'apparato hardware e software del Consorzio, potranno essere sperimentate nuove e migliori misure di protezione, tali comunque da non diminuire il livello di sicurezza individuato dal presente DPS. Dopo un periodo di sperimentazione da stabilirsi caso per caso, queste nuove misure di protezione potranno integrare quelle di cui al presente DPS, salvo poi venire recepite nel nuovo DPS in scadenza ogni anno. Nel caso invece queste nuove misure, seppur migliorative in termini di protezione e sicurezza, fossero in contrasto con i livelli individuati dal presente DPS, al termine della fase di sperimentazione e prima di quella di attuazione operativa, sarà necessario procedere ad una approvazione di un nuovo DPS.

Vengono innanzitutto identificati gli oggetti da proteggere:

- *dati*, distinguendo tra dati trattati con strumenti elettronici (file, record, cartelle) e dati trattati con altri strumenti (essenzialmente materiale cartaceo);
- *elementi di custodia* dei dati (arredi e hardware);
- *locali* ove sono ubicati gli elementi di custodia (uffici e sedi di lavoro in genere);

Di seguito vengono individuate le misure di protezione dei dati, degli elementi di custodia e dei locali, distinguendo tra le diverse categorie di rischio.

Dati

Dati - Dati trattati con strumenti elettronici

Dati - Dati trattati con strumenti elettronici - Rischio di distruzione o smarrimento dati

Nella sede centrale quotidianamente ciascun incaricato effettua una "sincronia" tra i files contenuti nel proprio hard disk e quelli contenuti in una apposita cartella "nominativa" (cioè riservata solo a quello specifico operatore ed alla quale ha accesso esclusivamente egli stesso, oltre all'amministratore di rete) su un server appositamente destinato al back-up (denominato server di back-up). In questo modo vengono duplicati tutti i dati contenuti nell'hard disk. Tra essi rientrano certamente tutti i dati trattati con programmi di Office automation nelle tre categorie individuate (Servizio sociale, Gestione personale, Contabilità).

Inoltre, 2 volte al giorno, il server di back-up acquisisce automaticamente dal server di dominio, il data base (di seguito db) del programma di contabilità e protocollo e di quello di rilevazione delle presenze.

Lo storage (archiviazione) del server si basa su una architettura denominata "raid 5" che permette la salvaguardia del contenuto di ogni hard disk, in caso di guasto fisico.

Nelle sedi periferiche, collegate al dominio tramite VPN (Virtual Private Network), dove ci sono più postazioni di lavoro in rete fra loro, settimanalmente tutti gli operatori effettuano una sincronia dei files del proprio hard disk, in una cartella nominativa sul server di back-up. In caso di limite di banda di connettività, questa operazione può avvenire anche di notte, tramite comandi automatizzati.

Nelle sedi periferiche non collegate in VPN con il dominio CISSA, settimanalmente viene effettuato un back up della parte di hard disk contenente dati, su un supporto rimovibile (cd rom, dvd rom o altro supporto), eventualmente riscrivibile.

Settimanalmente infine dal server di back-up viene effettuata automaticamente un back up su supporto rimovibile (cd rom, dvd rom, nastro o altro supporto) di tutte le cartelle

“nominative” presenti e dell’ultimo salvataggio disponibile del db di contabilità e protocollo, di quello di rilevazione delle presenze. e di eventuali altri applicativi. Il supporto rimovibile viene conservato all’esterno della struttura.

Per quanto riguarda i dati inseriti all’interno dalla procedura dei Servizi Sociali (di seguito definito applicativo “Modus”, dal nome originario della ditta fornitrice), l’operatore lavora attraverso il Terminal Server, sul data base unico contenuto all’interno del server di dominio, ubicato presso la sede centrale del CISSA.

Due volte al giorno il server di back- up acquisisce automaticamente dal server di dominio il db dell'applicativo Modus. Settimanalmente, dal server di back-up, viene effettuato un ulteriore back-up sul medesimo supporto rimovibile sopra indicato.

Si ritiene in questo modo di limitare complessivamente il rischio di irrimediabile distruzione o smarrimento dei dati.

Dati - Dati trattati con strumenti elettronici - Rischio di accesso non autorizzato

Per quanto riguarda il rischio di accesso non autorizzato, ogni pc è protetto da password di accesso di almeno 8 caratteri, da modificare almeno ogni 3 mesi con cronologia delle 4 password precedenti.

La password di amministratore di dominio è composta da almeno 12 caratteri, conformemente ai requisiti di complessità Microsoft.

Le password di accesso sono conosciute esclusivamente dall’utente. I soli responsabili di Area sono autorizzati a modificare le password di accesso ai pc in dotazione a dipendenti appartenenti alla propria Area, per esigenze di servizio, in mancanza dei dipendenti stessi. Il Direttore del Consorzio è autorizzato a modificare le password di accesso ai pc in dotazione ai responsabili di Area, per le medesime ragioni.

Nella sede centrale, ogni incaricato è responsabile del db contenuto nel proprio pc. In pratica, con questo sistema di autorizzazioni, ogni operatore accede esclusivamente al proprio db.

Nelle sedi periferiche, invece, si ritiene di individuare come unico db la somma dei files contenuti su tutti i pc presenti in ciascuna sede. Pertanto, ogni operatore deve poter accedere all’intero db, indipendentemente dalla conservazione di esso su un pc diverso da quello di abituale utilizzo. Ogni operatore è pertanto autorizzato ad accedere a tutti i pc della propria sede di lavoro.

E’ negato l’accesso a db di altre sedi.

Per l’accesso al db della procedura “Modus”, ogni operatore ha una propria password.

Anche per l’accesso al db di contabilità e protocollo gli operatori autorizzati dispongono di password personale.

Le password per l’accesso ai db di software specifici (contabilità e protocollo, altre eventuali procedure) sono conservate dal custode e dai vice custodi, mediante archiviazione delle stesse in un file protetto da password sul proprio pc. Ad ogni modifica di password da parte di uno o più incaricati, il file viene aggiornato. Per ragioni di praticità si ritiene di effettuare le modifiche password a scadenze predefinite, salve comunque esigenze di modifiche in tempi diversi, per ragioni di sicurezza.

Al fine di scongiurare il rischio di accesso durante le assenze temporanee dell’operatore, la password di accesso al pc viene impostata nelle proprietà dello schermo, in maniera tale che lo schermo proietti una maschera di sicurezza, subordinando l’accesso al sistema alla digitazione di tale password., qualora tale assenza si protragga oltre un certo numero di minuti predefiniti.

Dati - Dati trattati con strumenti elettronici - Rischio di trattamento con modalità non conformi a legge o regolamento

Per assicurare il trattamento dei dati in modalità conforme alla legge o regolamento vengono organizzati momenti formativi per ambiti lavorativi omogenei (p. es. per Area funzionale), nei quali il Responsabile del trattamento, o un soggetto da questi individuato, illustra le principali novità in tema di trattamento dati, siano esse originate da modifiche normative esterne (comunitarie, nazionali o regionali), siano esse frutto di innovazioni di regolamenti e/o disposizioni interne.

In ogni caso, almeno una volta all'anno è prevista una riunione (anche organizzata in moduli distinti per ambiti operativi omogenei), in tempi immediatamente successivi all'approvazione annuale del nuovo DPS, nella quale vengono illustrate le principali novità del Documento.

Il Responsabile del trattamento, direttamente o tramite soggetti da egli individuati in forma scritta (anche posta elettronica), effettua controlli, anche attraverso indagine a campione, sul rispetto delle modalità di trattamento dati. In caso di difformità rilevate, il Responsabile del trattamento adotta le opportune misure per porre rimedio, ove possibile, o limitare il danno. Ove si riscontri un inadempimento da parte di uno o più incaricati, viene avviato un procedimento disciplinare.

Qualora l'inadempimento comporti un danno di carattere economico, viene richiesto al soggetto inadempiente il risarcimento del danno patito.

Qualora la difformità del trattamento derivi da una carenza dal punto di vista normativo interno, anche di carattere interpretativo, il Responsabile del trattamento adotta le opportune contromisure (o ne propone l'adozione all'organo istituzionale competente).

Dati - Dati trattati con strumenti non elettronici

Dati - Dati trattati con strumenti non elettronici - Rischio di distruzione o smarrimento dati

Per supporti non elettronici si intendono principalmente i documenti cartacei.

I dati della "Gestione personale" sono in possesso anche della ditta che effettua l'elaborazione stipendi. Si tratta in pratica di buste paga, dichiarazione dei redditi e modulistica varia. Rappresenta tuttavia una parte residuale rispetto ai dati trattati con strumenti elettronici.

I dati della contabilità sono in possesso, oltre che del Consorzio, anche di alcuni fornitori di beni e servizi (in particolare le cooperative per la gestione di servizi alla persona e l'istituto di credito che gestisce il servizio di Tesoreria).

I dati del Servizio Sociale sono custoditi in luogo accessibile ai soli soggetti autorizzati, protetto con serrature. Inoltre, copia della modulistica su carta viene caricata su pc o server, aggiornando la procedura "Modus" o mediante file su pc.

In questo modo si ritiene di limitare in misura consistente il rischio di distruzione o smarrimento irrimediabile dei dati.

Dati - Dati trattati con strumenti non elettronici - Rischio di accesso non autorizzato

Tutti i documenti trattati con strumenti non elettronici sono archiviati in elementi di arredo quali armadi, cassetti, classificatori, dotati di idonea serratura.

Al termine di ogni giornata lavorativa ciascun incaricato ripone i documenti in questi mobili.

In caso di assenza prolungata dell'incaricato, nell'arco della stessa giornata di lavoro, questi deve provvedere a rimuovere dalla propria scrivania o altri piani d'appoggio i documenti cartacei contenenti dati personali e riporli nei mobili dell'ufficio, chiudendo con la chiave.

In caso di assenza dell'incaricato per più giorni, la posta ad egli destinata viene conservata in luogo sicuro e protetto da parte dell'operatore del protocollo, in attesa di consegnarla al suo rientro.

Dati - Dati trattati con strumenti non elettronici - Rischio di trattamento con modalità non conformi a legge o regolamento

Si applicano le medesime norme previste per il trattamento di dati con strumenti elettronici sopra individuate.

Elementi di custodia

Elementi di custodia - Rischio di distruzione o smarrimento degli elementi di custodia

In caso di distruzione degli elementi di custodia (siano essi elementi hardware, quali pc o server, o mobili per l'archivio cartaceo), la presenza di copie di back up, il caricamento della documentazione cartacea su file e la disponibilità dei documenti presso soggetti terzi (es. fornitori) limita alquanto la possibilità di perdita definitiva dei dati.

Elementi di custodia - Rischio di accesso non autorizzato

Per quanto riguarda gli strumenti elettronici, essi sono protetti da password di accesso, per cui, se rubati, non vi è rischio di accesso al db da parte del ladro. Allo stesso modo è impossibile accedere al db in caso di accesso furtivo o comunque non autorizzato ai pc.

Per quanto riguarda invece i mobili, il rischio derivante da un furto è scarso, anche se obiettivamente presente, in considerazione delle stesse dimensioni degli arredi.

L'accesso a singoli documenti cartacei o alle copie di back up di dati informatici archiviati su supporti rimovibili, invece, è protetto dai soggetti non autorizzati mediante chiusura a chiave dei mobili.

Una copia della chiave di ciascun mobile (ove sono conservati dati personali) è conservata, da parte dell'incaricato, all'interno del proprio ufficio o area di lavoro, in un mobile anch'esso chiuso a chiave.

Nella sede centrale l'incaricato, al termine della giornata lavorativa, trattiene la chiave di quest'ultimo mobile.

Una seconda copia della chiave di ciascun mobile è conservata all'interno dell'edificio in luogo sicuro da parte del custode delle password e di soggetti da questi individuati formalmente (anche tramite e-mail).

Nelle sedi distaccate del servizio sociale, invece, la chiave del mobile ove sono custodite le chiavi degli altri mobili, per ciascun ufficio, è riposta in un altro mobile individuato all'interno di ogni sede. Tutti gli incaricati al termine della giornata lavorativa, trattengono la chiave di quest'ultimo mobile.

Nei Centri Diurni a Valenza Educativa a gestione diretta, infine, le chiavi dei mobili contenenti dati personali sono conservate in un mobile individuato all'interno dell'edificio.

Una copia della chiave di quest'ultimo mobile è data in dotazione a tutti gli incaricati operanti in ciascuna sede.

Elementi di custodia - Rischio di trattamento con modalità non conformi a legge o regolamento

Viene assicurata la corretta informazione da parte del Responsabile del trattamento o da soggetti da questi individuati, analogamente a quanto precedentemente previsto per la protezione dei dati.

Per quanto riguarda i controlli, valgono le stesse regole precedentemente enunciate per quanto riguarda la protezione dei dati.

Locali

Locali – Rischio di distruzione

In caso di distruzione dei locali (crollo, incendio, ...), i dati trattati con strumenti elettronici (così come i dati contenuti in documenti cartacei caricati su pc) sono recuperabili attraverso copie di back up conservate presso strutture esterne al locale. Copie dei supporti rimovibili di back up custoditi presso la sede centrale sono conservati all'esterno della struttura, in luogo sicuro e protetto e distrutti o sovrascritti dopo circa 1 mese.

Per i dati contenuti in documenti cartacei conservati da società esterne, il rischio di distruzione o smarrimento irrimediabile non sussiste in quanto permane all'esterno del locale distrutto una copia del dato.

Locali - Rischio di accesso non autorizzato

Ogni incaricato ha in dotazione la chiave di accesso al locale, sede abituale di lavoro. Queste chiavi sono custodite con diligenza da parte del possessore.

In casi eccezionali, qualora un soggetto dell'amministrazione (ivi compresi i componenti degli organi di amministrazione e controllo) necessiti dell'accesso a locali diversi da quelli in cui lavora abitualmente (e dei quali pertanto è sprovvisto di chiave) in orari serali o durante le chiusure festive, il Responsabile del trattamento autorizza in forma scritta (anche mediante posta elettronica) il "temporaneo affidamento" della chiave di accesso al locale, specificando la durata di tale affidamento. Al termine del periodo di temporaneo affidamento, la chiave è restituita al Responsabile del trattamento, o al soggetto da questi individuato, previa attestazione di consegna e ricevuta.

Locali – Rischio di trattamento con modalità non conformi a legge o regolamento

Il Responsabile del trattamento cura l'informazione e vigila sul rispetto delle norme, nei modi previsti per la protezione dei dati, sopra descritti.

6 CRITERI DI RIPRISTINO DEI DATI A SEGUITO DI DISTRUZIONE O DANNEGGIAMENTO

In caso di distruzione o danneggiamento dei dati trattati con strumenti elettronici, si opera ripristinando dai back up effettuati la situazione aggiornata.

In caso di distruzione o danneggiamento dei dati trattati con strumenti non elettronici si opera come segue:

- se il documento cartaceo è archiviato, anche in forma sintetica, su file, si produce una copia di esso, attestandone la conformità all'originale da parte del Responsabile di Area competente ed indicando la data di riproduzione;
- se il documento non è archiviato su file poiché originato da altro soggetto (es. fornitore), si richiede a questi l'emissione di copia conforme del documento originale distrutto o danneggiato.

7 INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO

Oltre alla prevista riunione annuale sul nuovo DPS, in occasione di modifiche normative, si prevedono momenti formativi interni, ad opera di soggetti specializzati o dello stesso personale interno. Inoltre, vengono costantemente monitorate le offerte formative provenienti da soggetti specializzati.

In occasione di ogni modifica normativa o organizzativa (che non richieda apposita riunione illustrativa), il Responsabile del trattamento invia copia delle novità ai Responsabili di Area, al fine di coordinare con essi gli eventuali momenti formativi comuni o distinti per ambito organizzativo omogeneo.

8 CRITERI PER GARANTIRE IL RISPETTO DI MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTI DI DATI PERSONALI AFFIDATI A SOGGETTI ESTERNI ALL'AMMINISTRAZIONE

I soggetti cui vengono affidati dati raccolti dal Consorzio vengono nominati "Responsabile al trattamento dati per dati trattati all'esterno".

Per quanto riguarda gli appalti, negli atti preliminari di gara deve farsi espresso richiamo, qualora possibile e pertinente, al DPS del Consorzio, come ad una norma interna da rispettare. In questo caso, con la presentazione dell'offerta le ditte implicitamente accettano il DPS del Consorzio o allegano il proprio (servendosi anche di supporti magnetici quali floppy disk, cd rom, ...), dichiarandone l'equivalenza in termini di tutela dei dati personali, consentendo così uno snellimento dell'iter sopra definito.

In caso di dichiarazione di equivalenza del proprio DPS a quello del Consorzio, prima dell'aggiudicazione definitiva del servizio o fornitura ed in ogni caso prima della nomina di Responsabile del trattamento per dati trattati all'esterno, il Responsabile del trattamento del Consorzio, di concerto con il Responsabile di Area competente, esaminano l'eventuale DPS della ditta provvisoriamente aggiudicataria e ne confermano l'equivalenza con quello del Consorzio o dispongono eventuali misure aggiuntive, dandone comunicazione scritta alla ditta, entro 10 giorni dall'aggiudicazione provvisoria. In caso di rifiuto ad adottare il DPS del Consorzio o le disposizioni aggiuntive, da comunicare in forma scritta entro altri 10 giorni, l'aggiudicazione provvisoria s'intende revocata e si provvede allo scorrimento della graduatoria dell'appalto o all'indizione di una nuova procedura di gara.

In caso poi, nel corso dello svolgimento del servizio o della fornitura (specie se continuativa) di beni, la ditta non osservi le norme del DPS del Consorzio o le proprie dichiarate e confermate come equivalenti, e pregiudichi la tutela dei dati ad essa affidati, vengono applicate le penalità previste dal capitolato d'appalto (o dagli altri atti di gara), graduate in relazione alla gravità dell'inadempimento, oltre all'eventuale richiesta di risarcimento dei danni causati.

Nei casi più gravi può disporsi la revoca dell'affidamento e l'eventuale denuncia alle competenti autorità per l'avvio di un procedimento legale.