Consorzio Padule di Fucecchio

ELENCO DELIBERE DEL COMMISSARIO STRAORDINARIO DEL 20 APRILE 2011		
Numero	**Data**	
51.	**20.04.11**	**"INTERVENTI IDRAULICO FORESTALI NEL COMUNE DI CAPRAIA E LIMITE SULL'ARNO (ZONA G)" - C.R.E. E ATTI DI COLLAUDO - APPROVAZIONE**
52.	**20.04.11**	**AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (D.P.S.) AI SENSI DEL D. LGS. 196/2003 - PROVVEDIMENTI -**
53.	**20.04.11**	**GARA D'APPALTO DEI LAVORI DI "MANUTENZIONE ORDINARIA PER L'ANNO 2011 DEGLI IMPIANTI CONSORTILI"- AGGIUDICAZIONE –**

Sede: 51019 PONTE BUGGIANESE (Pistoia) - Via Libertà, 28 - Tel. 0572/93221 - Fax 0572/634527
Web: www.paduledifucecchio.it e-mail: info@paduledifucecchio.it

DELIBERAZIONE n. **51** del **20 APRILE 2011**

"INTERVENTI IDRAULICO FORESTALI NEL COMUNE DI CAPRAIA E LIMITE SULL'ARNO (ZONA G)"
- C.R.E. e ATTI DI COLLAUDO - APPROVAZIONE

IL COMMISSARIO STRAORDINARIO

PREMESSO

1. CHE con deliberazione n. 54 del 17.04.2009 la Deputazione Amministrativa ha approvato il progetto esecutivo di *"Interventi idraulico forestali nel Comune di Capraia e Limite sull'Arno (zona G)"* per l'importo complessivo di € 50.000,00;
2. CHE con Atto di Affidamento in data 14.05.2009 rep. n° 592, registrato a Pescia il 18.05.2009 al n°1799 Serie III i lavori sono stati affidati alla ditta "Consorzio Cooperative Forestali Toscana Verde (CTV)" con sede in Castelnuovo Garfagnana (LU), via E. Fermi n.27, P.I. 00787960525;
3. CHE il "Consorzio Cooperative Forestali Toscana Verde (CTV)" ha dichiarato come impresa esecutrice dei lavori la cooperativa associata "Sole Società Cooperativa Sociale ONLUS" con sede in Capraia Fiorentina (FI), via S. Carnevale n. 35, P.I. 04990750483;

CONSIDERATO che i lavori stessi sono stati ultimati e contabilizzati;

VISTO il Certificato di Regolare Esecuzione nei rapporti fra questo Consorzio di Bonifica, Ente appaltante e l' impresa esecutrice, a firma del Direttore dei Lavori Ing. Junior Cristiano Nardini, in data 04.06.2010 dal quale risulta che l'importo netto complessivo dei lavori eseguiti ammonta ad € 40.104,28 compresi oneri di sicurezza, oltre IVA;

VISTA la proposta di deliberazione presentata in data 20 aprile 2011 dal Responsabile del Settore "Opere" Dott. Ing. Lorenzo Galardini;

VISTO il parere di regolarità contabile rilasciato dal Responsabile del "Settore Amministrativo" Dott. Riccardo Ferri in data 20 aprile 2011;

VISTO il parere di legittimità presentato in data 20 aprile 2011 dal Direttore Generale del Consorzio Dott. Franco Fambrini;

RITENUTA la regolarità degli atti;

D E L I B E R A

APPROVARE il Certificato di Regolare Esecuzione dei lavori di "*Interventi idraulico forestali nel Comune di Capraia e Limite sull'Arno (zona G)*", e gli Atti di Collaudo a firma del Direttore dei Lavori Ing. Junior Cristiano Nardini nei rapporti fra Consorzio di Bonifica, Ente appaltante ed impresa esecutrice per l'importo complessivo netto dei lavori pari ad € 40.104,28;

ORDINARE il pagamento, per i titoli di cui sopra, a favore dell'Impresa "Consorzio Cooperative Forestali Toscana Verde (CTV)" con sede in Castelnuovo Garfagnana (LU), via E. Fermi n.27, P.I. 00787960525, dell'importo complessivo di € 240,62 di cui € 200,52 per lavori e sicurezza (trattenute di legge in ragione dello 0,5%) e € 40,10 per IVA;

IMPUTARE la spesa al CAPITOLO 240/R (impegno 09/50225) del bilancio dell'esercizio in corso.

IL COMMISSARIO STRAORDINARIO
(Rag. Gino Biondi)

Consorzio di Bonifica Padule di Fucecchio

DELIBERAZIONE n. **52** del **20 APRILE 2011**

AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (D.P.S.) AI SENSI DEL D. LGS. 196/2003 - PROVVEDIMENTI -

IL COMMISSARIO STRAORDINARIO

PREMESSO che con deliberazione n. 112 del 30/08/2005 è stato approvato il Documento Programmatico sulla Sicurezza (D.P.S.) e dei relativi allegati predisposto ai sensi del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali);

CONSIDERATO:
- che il sopra citato D. Lgs. 196/2003 prevede l'aggiornamento annuale del D.P.S.;
- che, pertanto, si rende necessario approvare il D.P.S. aggiornato al mese di marzo 2011;

VISTO il documento di aggiornamento al D.P.S. allegato al presente atto;

VISTA la proposta di deliberazione presentata in data 20 aprile 2011 dal Responsabile del Settore "Amministrativo" Dott. Riccardo Ferri;

VISTO il parere di legittimità presentato in data 20 aprile 2011 dal Direttore Generale del Consorzio Dott. Franco Fambrini;

RITENUTA la regolarità degli atti;

D E L I B E R A

APPROVARE il documento di aggiornamento del D.P.S. come riportato nelle premesse che, allegato al presente atto, forma parte integrante e sostanziale dello stesso.

IL COMMISSARIO STRAORDINARIO
(Rag. Gino Biondi)

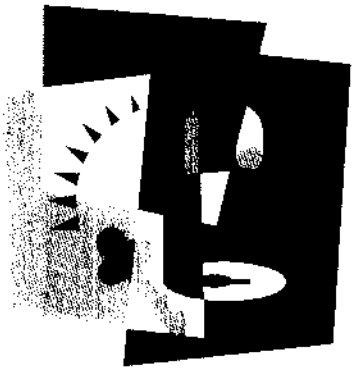
Sede: 51019 PONTE BUGGIANESE (Pistoia) - Via Libertà, 28 - Tel. 0572/93221 - Fax 0572/634527
Web: www.paduledifucecchio.it e-mail: info@paduledifucecchio.it

DOCUMENTO PROGRAMMATICO

SULLA SICUREZZA

AGGIORNAMENTO

MARZO 2011



Decreto Legislativo 30 giugno 2003, n. 196,

modificato dall'art. 29 del Decreto Legge 26.06.2008 n. 112, conv. con modif. nella Legge 06.08.2008, n. 133

e

Allegato B) – Disciplinare Tecnico in materia di misure di sicurezza

SOMMARIO

Allegati

a) ---------- (inserito nella parte I, punto 3: schema rete)

b) ---------- (inserito nella parte I, punto 1: censimento archivi)

c) Mansionario Privacy

d) Nomine Responsabili **(aggiornata)**, Nomina custode passwords (all. al DPS ed. "0"), Lettere incarico **(aggiornata)**

e) ---------- (inserito nella parte II, punto 1: tabella riepilogativa rischi)

f) Piano di formazione (all. al DPS ed. "0")

g) Piano di verifica misure adottate **(aggiornato)**

h) Regolamento informatico consortile (all. al DPS ed. "0")

i) Annotazione sulla relazione di bilancio (all. al DPS ed. "0")

j) Clausola e dichiarazione di conformità (all. al DPS ed. "0")

k) Nomina medico competente (all. al DPS ed. "0")

l) Lettera per prestatori di servizi sull'applicazione misure di sicurezza (all. al DPS ed. "0")

m) Informative ai fornitori, dipendenti, per curricula, consorziati, utenti (all. al DPS ed. "0")

n) Lettera ditta di pulizie **(aggiornata)**

o) Clausola per giornalino consortile (all. al DPS ed. "0")

p) Lettera nomina Amministratore di sistema **(aggiornata)**;

q) Informativa videosorveglianza;

r) Lettera incarico videosorveglianza.

Procedure

PGR01 - Trattamenti con strumenti elettronici

PGR02 - Trattamenti senza strumenti elettronici

PGR03 - Videosorveglianza

Premessa

Il presente Documento Programmatico sulla Sicurezza (DPS) costituisce **l'aggiornamento per il 2011** del DPS già redatto negli anni precedenti, come riportato nell'indice delle revisioni riportate alla fine del paragrafo.

Nella redazione dell'aggiornamento, sono state considerate ed esaminate le modifiche normative intervenute più recenti, oltre che i Provvedimenti di carattere generali emanati dal Garante per la protezione dei dati personali, di interesse del titolare, che qui di seguito si riportano per completezza.

Fonte	Rubrica / oggetto
D.L. 25 giugno 2008, n. 112 conv. con modif. in legge 6 agosto 2008, n. 133 (inserimento comma 1-bis, all'art. 34, D.Lgs. n. 196/2003, Art. 34 - Trattamenti con strumenti elettronici)	*Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione Tributaria*
D.L. 30 dicembre 2008, n. 207, conv. con modif. in legge 27 febbraio 2009, n. 14	*Proroga di termini previsti da disposizioni legislative e disposizioni finanziarie urgenti*
LEGGE 4 marzo 2009, n. 15 (art. 4, comma 9)	*Delega al Governo finalizzata all'ottimizzazione della produttività del lavoro pubblico e alla efficienza e trasparenza delle pubbliche amministrazioni nonché disposizioni integrative delle funzioni attribuite al Consiglio nazionale dell'economia e del lavoro e alla Corte dei conti*

Prescrizione del Garante per la protezione dei dati personali del 19 giugno 2008	*Semplificazione di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili*
Provvedimento a carattere generale del 27 novembre 2008 – Garante per la protezione dei dati personali	*Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali*
Provvedimento a carattere generale del 27 novembre 2008 – Garante per la protezione dei dati personali	*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*
Comunicato stampa Garante - 10 dicembre 2009	*Amministratori di sistema: precisazioni del Garante*

Il documento, che ha coinvolto nella sua redazione i responsabili nominati dall'ente, si prefigge l'obiettivo di contribuire al miglioramento della gestione della sicurezza nel Consorzio anche attraverso una crescita culturale, a tutti i livelli, della sicurezza dei dati. Il documento, in **edizione "5.1" (cd. aggiornamento)**, è considerato come un documento di base, strumento per il titolare del trattamento da aggiornare in base all'evoluzione "aziendale" e tecnica, tenendo sempre presente il principio che la sicurezza dei dati è un processo continuo, integrato, che correla gli aspetti organizzativi, procedurali, tecnici, informatici e logistici.

L'**edizione "5.1"** del documento aggiorna e sostituisce il precedente aggiornamento **"4.1"**. Infatti, il Disciplinare tecnico prevede che **entro il 31 marzo di ogni anno il titolare di un trattamento di dati sensibili o di dati giudiziari rediga anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza (punto 19).**

Il Codice sulla Privacy (D. Lgs. n.196/2003) impone a tutti coloro che trattano dati personali la predisposizione di adeguati controlli e misure in materia di sicurezza, sulla base di uno specifico protocollo previsto dal cosiddetto Disciplinare Tecnico in materia di misure minime di sicurezza (allegato B del citato Decreto Legislativo), come già rilevato nelle precedenti edizioni del Documento Programmatico sulla Sicurezza.

Si ricorda che il titolare del trattamento, oltre agli adempimenti già in essere in quanto previsti dalla precedente disciplina (tra le altre, la Legge 675 del 31 dicembre 1996) quali, ad esempio, l'informativa, la preventiva richiesta del consenso quando prevista, deve adottare, oltre che misure minime, anche misure di sicurezza idonee, in quanto i dati personali devono essere custoditi e controllati in modo da ridurre ragionevolmente il rischio di sottrazione o perdita degli stessi, nonché di accessi non autorizzati da parte di terzi, evitando inoltre il trattamento di dati non consentito e non conforme.

Infatti, il legislatore richiede l'utilizzo di quanto il progresso tecnologico e scientifico mette continuamente a disposizione nel tempo, conseguentemente le misure che potevano considerarsi in un certo momento storico idonee a garantire la protezione e la sicurezza dei dati personali, possono ritenersi insufficienti o comunque non idonee oggi.

Il "documento programmatico sulla sicurezza" rappresenta sempre una sorta di manuale della sicurezza ai fini del trattamento dei dati personali tutelati dal "Codice sulla Privacy".

Tale documento assume un ruolo fondamentale nella pianificazione di ogni scelta di sicurezza effettuata dal titolare del trattamento dei dati personali, il **Consorzio di Bonifica del Padule di Fucecchio,** più avanti identificato.

Il DPS rimane suddiviso, come **nella precedente edizione**, in tre parti con **alcune varianti** principalmente nell'organigramma degli incaricati, nonché nella previsione della **nuova Procedura 03 relativa alla videosorveglianza, considerata l'installazione di tre telecamere a partire da Aprile 2010.**

La prima parte, dedicata alla situazione dell'ente attuale, inizia con l'elenco dei trattamenti dei dati personali effettuati dal titolare, per proseguire con la descrizione della distribuzione dei compiti e delle responsabilità all'interno ed all'esterno della struttura. Successivamente, viene descritto il sistema informatico presente nella struttura, sia nelle sue componenti hardware che in quelle software. Tutto ciò al fine di poter meglio evidenziare i rischi che incombono sui dati.

Nella seconda parte sono esplicitate le misure di sicurezza adottate e quelle che si intendono adottare al fine di garantire un adeguato livello di protezione dei dati personali di cui si effettua il trattamento, in conformità a quanto richiesto dal D.Lgs. n. 196/2003. Viene riportata all'interno del DPS la tabella riepilogativa dei rischi.

La terza parte concerne la formazione obbligatoria degli incaricati al trattamento e l'adeguamento annuale del DPS.

Si ricorda che la redazione del DPS rappresenta un adempimento di primaria importanza per il Consorzio, la cui mancata osservanza (come peraltro la mancata adozione delle altre misure minime) fa incorrere il titolare, o anche il responsabile eventualmente delegato, nel reato contravvenzionale di cui all'art. 169 (arresto sino a due anni).

Oltre che un adempimento minimo obbligatorio, il DPS rappresenta, comunque, una misura opportuna per analizzare la situazione dell'ente, ottimizzarne l'organizzazione, ed un'occasione per delineare una idonea politica sulla sicurezza.

Campo di applicazione

Il presente Documento Programmatico sulla Sicurezza definisce le politiche e gli standard di sicurezza definiti dal titolare in merito al trattamento di tutti i dati personali effettuati in azienda.

Esso riguarda il trattamento dei seguenti dati personali:

- Comuni
- Sensibili
- Giudiziari

Inoltre, si applica al trattamento di tutti i dati personali effettuato per mezzo di:

- Strumenti elettronici
- Altri strumenti di elaborazione (ad esempio, cartacei, etc.)

Il Documento Programmatico sulla sicurezza deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

Definizioni

TRATTAMENTO

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di

dati, anche se non registrati in una banca di dati.

DATO PERSONALE

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI

Dati personali che permettono l'identificazione diretta dell'interessato.

DATI SENSIBILI

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, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DATI GIUDIZIARI

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 qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

TITOLARE

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.

RESPONSABILE

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

INCARICATI

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

INTERESSATO

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

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.

DIFFUSIONE

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

DATO ANONIMO

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

BLOCCO

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

BANCA DI DATI

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

GARANTE

L'autorità di cui all'articolo 153 D. Lgs. n. 196/2003, istituita dalla legge 31 dicembre 1996, n. 675.

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.

MISURE MINIME

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

STRUMENTI ELETTRONICI

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

AUTENTICAZIONE INFORMATICA

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

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

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.

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.

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.

Indice delle revisioni

Revisione	Data redazione	Firma titolare
0	02.04.2005	Biondi Gino
1.1	27.03.2007	Biondi Gino
2.1	25.03.2008	Biondi Gino
3.1	31.03.2009	Biondi Gino
4.1	31.03.2010	Biondi Gino
5.1	31.03.2011	Biondi Gino

PARTE Iª
ANALISI DELLA SITUAZIONE DELL'ENTE

1. Analisi dei trattamenti dei dati personali (punto 19.1 Disciplinare tecnico)

Sono stati nuovamente esaminati tutti i trattamenti di dati personali effettuati dal titolare, il **Consorzio di Bonifica del Padule di Fucecchio** (Disciplinare tecnico allegato al d.lgs. n. 196/2003), che svolge le seguenti attività:

ELENCO ATTIVITA' ESERCITATE

- Il Consorzio gestisce, progetta opere ed infrastrutture atte a garantire e sviluppare la bonifica idraulica e l'irrigazione.

  In particolare, l'ente si occupa della manutenzione delle opere idrauliche, della tutela dal rischio idraulico e della tutela ambientale, oltre che delle altre funzioni previste dallo Statuto consortile.

Tale analisi è stata effettuata prendendo come documento di base il censimento degli archivi individuato nell'aggiornamento del DPS in **edizione 4.1, rimasto invariato. Si precisa che la custodia dei documenti amministrativi, tecnici e catastali, dalla costituzione dell'ente fino all'anno 2006, nei locali adibiti ad archivio ubicato in Via Perosi, n. 14/16. Gli ultimi cinque anni sono conservati presso la sede del Consorzio.**

Si evidenzia che il ruolo degli incaricati del Consorzio si riconduce alle seguenti aree funzionali in relazione alle quali sono stati censiti i diversi trattamenti di dati effettuati. Si specifica che è stato abolito il Settore Aree Protette.

Direzione Generale	Direzione Generale	
Area Amministrativa	Settore Amministrativo	
	Settore Catasto	
Area Tecnica	Settore Opere	Sezione manutenzione opere

E' di fondamentale rilievo ricordare che la definizione di **trattamento** è molto ampia. Infatti, ai sensi dell'art. 4, lett. a), del Codice sulla Privacy, si intende per "trattamento qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca dati".

Il Consorzio ha **aggiornato** il censimento dei singoli trattamenti individuando le banche dati trattate, la natura dei dati personali in esse contenuti, nonché le finalità e modalità del trattamento ed i soggetti ai quali vengono comunicati i dati, in corrispondenza di ogni area funzionale.

L'elenco dei trattamenti di dati personali e sensibili effettuato dal Consorzio viene riportato qui di seguito, **aggiornato con la soppressione del Settore Aree Protette.**

DIREZIONE GENERALE

ELENCO DATI PERSONALI TRATTATI

Ufficio	Banca Dati - Natura dati	Interessati	Modalità trattamento	Finalità trattamento	Luogo dove sono conservati	A chi vengono comunicati
Direzione Generale	Tutti i dati	Cfr. Aree specifiche	Cartaceo ed informatico	Superivisione e coordinamento	Armadi e scaffali presso le Aree e Server	Cfr. Aree specifiche

AREA AMMINISTRATIVA

SETTORE AMMINISTRATIVO

ELENCO DATI PERSONALI TRATTATI

Banca Dati - Natura dati	**Interessati**	**Modalità trattamento**	**Finalità trattamento**	**Misure di sicurezza e protezione dei dati**	**Luogo dove sono conservati**	**Personale che ha accesso ai dati**	**A chi vengono comunicati/ Outsourcers**
Archivio protocollo - dati personali, sensibili e giudiziari	Mittenti varie e destinatari	Cartaceo ed informatico	Conservazione /estrazione corrispondenza spedita e ricevuta	Armadi chiusi a chiave / password	Informatico :Server Cartaceo: stanza archivio 2°piano e archivio esterno adiacente alla sede **(V.Perosi 14/16)**	Settore amministrativo, incaricati di competenza	Consulente software protocollo
Archivio atti - dati personali	Amministratori per i verbali e sogg. Vari presenti nelle delibere (imprese, contribuenti, etc.)	Cartaceo ed informatico	Conservazione /estrazione deliberazioni Deputazione Amministrativa, Consiglio dei delegati e commissioni	Armadi / password	Informatico :Server Cartaceo: stanza armadio ufficio direttore	Settore Catasto e amministrativo, incaricati di competenza	Consulente Sito Web
Archivio clienti e fornitori - dati personali	Clienti e fornitori	Cartaceo ed informatico	Adempimenti contabili	Password	Informatico :Server Cartaceo: Settore amministrativo	Settore amministrativo	Tesoriere, Consulente software programma di contabilità
Archivio mandati e reversali e documentaz allegata - dati personali e sensibili.	Beneficiari pagamenti e soggetti versanti	Cartaceo (con allegati) ed informatico (senza allegati)	Conservazione /estrazione mandati e reversali	Armadi chiusi a chiave e password	Informatico :Server Cartaceo: armadio chiuso a chiave stanza ufficio ragioneria e archivio esterno adiacente la sede consortile	Settore amministrativo	Tesoriere

					(V.Perosi 14/16)		
Archivio schede personale dipendente - dati personali, sensibili e giudiziari	Personale dipendente	Cartaceo	Adempimenti contrattuali e legali relativi al personale	Chiusura a chiave	Cartaceo: cassaforte ufficio del Commissario e ufficio ragioneria	Settore amministrativo, Direzione	
Archivio amministratori - dati personali	Amministratori	Cartaceo ed informatico	Adempimenti relativi ai pagamenti degli amministratori	Armadi chiusi a chiave e password	Informatico :Server Cartaceo: armadio chiuso a chiave e ufficio ragioneria	Settore amministrativo	Tesoriere, Consulente del lavoro e Società elaborazione compensi
Archivio dipendenti (deleghe sindacali, certificati medici, etc.) - dati personali, sensibili e giudiziari	Personale dipendente	Cartaceo ed informatico	Adempimenti contabili e fiscali	Chiusura a chiave	Informatico :Server Cartaceo: Armadio chiuso a chiave Ufficio Ragioneria e Personale	Settore amministrativo	Consulente del lavoro e Società elaborazione compensi
Archivio presenze - dati personali, sensibili	Personale dipendente	Cartaceo	Adempimenti contabili e fiscali	Chiusura a chiave	Cartaceo: Armadio chiuso a chiave Ufficio Ragioneria e Personale	Settore amministrativo	Consulente del lavoro e Società elaborazione compensi
Archivio informative e consenso - dati personali	Interessati	Cartaceo	Adempimenti privacy	Chiusura a chiave	Cartaceo: Armadio chiuso a chiave Ufficio Ragioneria e Personale	Settore amministrativo	Consulente del lavoro e Società elaborazione compensi

AREA AMMINISTRATIVA

SETTORE CATASTO

ELENCO DATI PERSONALI TRATTATI

Banca Dati - Natura dati	Interessati	Modalità trattamento	Finalità trattamento	Misure di sicurezza e protezione dei dati	Luogo dove sono conservati	Personale che ha accesso ai dati	A chi vengono comunicati/ Outsourcers
Archivio consorziati - dati personali	Consorziati	Cartaceo ed informatico	Gestione ruoli	Armadi / password	Informatico :Server Cartaceo: stanza uffici catasto piano terra	Settore catasto	Consulente software, Concessionari della riscossione, Catasto.

AREA TECNICA

SETTORE OPERE E SETTORE TECNICO/AMMINISTRATIVO

ELENCO DATI PERSONALI TRATTATI

Banca Dati - Natura dati	Interessati	Modalità trattamento	Finalità trattamento	Misure di sicurezza e protezione dei dati	Luogo dove sono conservati	Personale che ha accesso ai dati	A chi vengono comunicati/ Outsourcers
Archivio lavori - dati personali ,	Imprese, sogg. vari interessati ai lavori eseguiti. In particolare soggetti espropriati e da espropriare	Cartaceo ed informatico	Adempimenti tecnici, predisposizione progetti, contabilità lavori	Armadi / password	Informatico :Server Cartaceo: ufficio tecnico	Area tecnica	Consulente software Contabilità lavori, Notaio (atti di esproprio), Enti concessionari di opere

L'importanza del censimento, richiesto dal punto 19.1 del Disciplinare tecnico, è dovuta al fatto che il livello di cautele da adottare per predisporre le misure di sicurezza idonee e minime varia a seconda della tipologia di dati che vengono trattati.

Tali misure, infatti, devono assumere un carattere crescente a seconda che si trattino dati personali comuni, sensibili e giudiziari.

I documenti su supporto cartaceo vengono ordinatamente raccolti nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, e comunque a fine giornata, in armadi/scaffali/uffici sopra individuati e in un locale chiuso a chiave quando riguardano dati sensibili e giudiziari.

È risultato, quindi, necessario verificare le applicazioni esistenti e, sulla base delle informazioni assunte, determinare se attraverso le stesse il Consorzio effettua il trattamento dei dati personali secondo quanto previsto dal Codice sulla privacy.

Lo **Scopo** dell'analisi è stato quello di inventariare e "mappare" gli archivi contenenti dati personali e verificare la conformità del loro trattamento alle disposizioni normative.

L'**Oggetto** dell'analisi inventariale sono stati tutti i trattamenti effettuati, con o senza l'ausilio di strumenti elettronici, attraverso una descrizione sommaria ma esplicativa dei contenuti, delle finalità e modalità del trattamento.

Sulla base delle informazioni ottenute dai responsabili ai referenti in materia di privacy, e di quanto previsto dall'art. 37 d.lgs n. 196/2003, sono stati nuovamente esaminati i trattamenti effettuati allo scopo di chiarire se gli stessi siano soggetti a Notifica al Garante.

Sulla base delle evidenze emerse si è esclusa la necessità di effettuare la notificazione (si veda anche: Provvedimento a carattere generale del Garante n.1/2004 del 31 Marzo 2004, in Gazzetta Ufficiale del 6 aprile 2004, n. 81).

2. La distribuzione di compiti e responsabilità all'interno ed all'esterno della struttura (punto 19.2 Disciplinare tecnico)

In relazione ai trattamenti effettuati e sopra indicati, è ora necessario descrivere l'organizzazione della struttura di riferimento, individuando i compiti e le relative responsabilità dei soggetti interessati nel trattamento dei dati personali.

Nella struttura essenziale, l'organigramma del Consorzio è **in parte variato** rispetto alla redazione dell'aggiornamento del DPS in **edizione 4.1, nella parte relativa agli incaricati del trattamento.**

Si ricorda che il Garante per la protezione dei dati personali, con il **Provvedimento di 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), prescrive a tutti i

titolari dei trattamenti dei dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, salvo quelli che siano stati oggetto delle misure di semplificazione, nuovi adempimenti e misure relativamente alla figura dell'**amministratore di sistema.**

Il Garante riconosce, infatti, che l'individuazione di soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti.

Con la definizione di **amministratore di sistema** si individuano generalmente, in ambito informatico, **figure professionali finalizzate alla gestione e manutenzione di un impianto di elaborazione o di sue componenti.** Ai fini del Provvedimento in esame, il Garante considera tali anche altre **figure equiparabili** dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di base di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Nel caso in cui l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, il titolare, nella qualità di datore di lavoro, deve rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito della propria organizzazione, in relazione ai diversi servizi informatici cui questi sono preposti.

Le disposizioni specifiche in materia di organizzazione interna contenute nel Codice, relative alle figure del Responsabile (art. 29) e dell'Incaricato (art. 30) al trattamento dei dati personali, sono rimaste invariate.

Alla luce di ciò, qui di seguito sono stati individuati i soggetti coinvolti nel trattamento dei dati personali, secondo le disposizioni riportate nel mansionario, aggiornato con la nuova figura dell'amministratore di sistema, che definisce i ruoli, descrive i compiti e conseguentemente le responsabilità sancite dal d. lgs. n. 196/2003 nell'ambito delle figure preposte al trattamento dei dati.

Si ricorda che il **titolare** è 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 (art. 4, comma 1, lett. f).

Nel caso di specie, il "titolare del trattamento" dei dati è il **Consorzio di Bonifica del Padule di Fucecchio** (81002610475), con sede in Ponte Buggianese (PT) Via Libertà 28, il cui legale

rappresentante è il Sig. Biondi Gino (c.f. BNDGNI54P06G713Q), nato a Pistoia (PT) il 06-09-1954, e residente in MONTECATINI TERME (PT) Via G. di Vittorio, 26.

Il dettato normativo chiarisce, infatti, che nel caso in cui il trattamento venga effettuato da una persona giuridica, da una pubblica amministrazione o da un altro ente, associazione od organismo, titolare è ***l'entità nel suo complesso***, o l'organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza (art. 28), anziché la persona fisica incardinata nell'organo o preposta all'ufficio.

I dati identificativi del titolare del trattamento sono i seguenti:

Ragione sociale:	**Consorzio di Bonifica del Padule di Fucecchio**
Indirizzo della sede legale:	Via Libertà nr. 28 Ponte Buggianese (PT)
Telefono:	**0572.93221**
Fax:	0572.634527
E-mail:	**info@paduledifucecchio.it**
PEC:	**consorzio@pecpaduledifucecchio.it**
Partita IVA:	-
Codice Fiscale:	**81002610475**
Unità locale ad uso archivio	**Via Perosi nr. 14/16 - Ponte Buggianese (PT)**

Il T.U. privacy prevede la possibilità per il titolare di designare facoltativamente uno o più responsabili del trattamento dei dati, interni od esterni all'ente, al fine di razionalizzarne la struttura e l'organizzazione, delegando parzialmente compiti e conseguentemente responsabilità (civili, amministrative e penali).

Secondo la definizione fornita dal decreto all'art. 4, comma 1, lett. g), il **responsabile** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposto dal titolare al trattamento dei dati personali.

Premesse tali definizioni e preso atto che il responsabile del trattamento deve essere 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", il Consorzio di Bonifica ha ritenuto di continuare ad avvalersi come **responsabili interni** delle figure qui di seguito indicate:

Come responsabile del trattamento è **confermato** il **Dott. Riccardo Ferri** *(FRRRCR76M01G713T)*, nato a Pistoia il 01-08-1976, e dipendente del Consorzio inquadrato nell'Area Amministrativa,

domiciliato per la funzione presso la sede del Consorzio. La nomina è stata aggiornata con le prescrizioni in ordine al sistema di videosorveglianza installato.

Come responsabile delle misure di sicurezza informatiche è **confermato** il ***Sig. Massimo Anzilotti*** *(NZLMSM64D18E715K),* nato a Lucca il 18-04-1964, e dipendente del Consorzio inquadrato nell'Area Amministrativa, domiciliato per la funzione presso la sede del Consorzio.

Il Consorzio ha già integrato la nomina del sig. Anzilotti Massimo, con l'incarico di **Amministratore di sistema, aggiornata nel 2011 con le prescrizioni in ordine al sistema di videosorveglianza installato.**

Tale decisione dell'ente è stata presa a fronte del Provvedimento generale del Garante del 27 novembre 2008 richiamato sopra, dal titolo *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*.

Il Consorzio ha infatti valutato preventivamente l'esperienza, la capacità e affidabilità del Sig. Anzilotti, ritenendo che abbia fornito idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

L'elenco delle mansioni del Sig. Anzilotti vengono riportate qui di seguito, come richiesto dal Provvedimento generale del Garante appena indicato e verranno riportate nella lettera di nomina, allegata al Documento Programmatico sulla sicurezza, costituendone parte integrante, alla stessa stregua delle altre lettere di nomina dei responsabili e incaricati.

L'amministratore di sistema ha prevalentemente il compito di:

- **assegnare ad ogni incaricato del trattamento l'opportuno profilo (credenziali di autenticazione ed autorizzazione) e successivamente impartire agli incaricati le istruzioni scritte necessarie per un corretto, lecito, sicuro utilizzo degli strumenti elettronici. Le istruzioni dovranno essere integrate con le adeguate prescrizioni sulle misure di sicurezza da applicare definite ed analizzate nelle procedure allegate al DPS adottato dal Consorzio;**
- assegnare e gestire i codici identificativi personali prevedendone la disattivazione nel caso di perdita della qualità che consente all'incaricato l'accesso all'elaboratore e ai dati personali, ovvero nel caso di loro mancato utilizzo per un periodo superiore a sei mesi;
- **vigilare sul rispetto delle istruzioni impartite e delle misure di sicurezza da parte degli incaricati;**
- predisporre ed aggiornare le misure di sicurezza prescritte dagli articoli 31 - 35 del d. lgs. n.196/2003 e dall'allegato B) al decreto stesso (Disciplinare tecnico in materia di misure di sicurezza), ottemperando, in particolare, a quanto previsto dal documento programmatico sulla sicurezza, curandone l'applicazione da parte degli incaricati;
- **assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di**

autorizzazione in uso nel Consorzio, valutando il sistema più idoneo e sicuro da utilizzare informandone il custode delle passwords;

- predisporre e rendere funzionanti le copie di sicurezza (operazioni di back up e disaster recovery) dei dati e delle applicazioni.
- **disporre ogni opportuna misura e ogni adeguata verifica, per evitare che soggetti non autorizzati possano avere accesso agli archivi delle parole chiave;**
- provvedere affinché gli elaboratori del sistema informativo siano protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615 quinquies c.p., mediante idonei programmi la cui efficacia ed aggiornamento siano verificati con cadenza almeno semestrale;
- **assistere il Responsabile del trattamento in particolare per quanto concerne l'analisi dei rischi presso la propria Struttura e per le informazione che il Responsabile è tenuto ad inviare al Titolare per la stesura annuale del Documento Programmatico di Sicurezza (DPS);**
- adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici degli amministratori di sistema.
  Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, 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.
- **adempiere ad ogni altro obbligo previsto dalla normativa vigente, comunicando immediatamente al titolare eventuali nuove misure di sicurezza da adottare..**
- **In particolare, relativamente al sistema di videosorveglianza installato (si veda PGR03, allegata al presente DPS), l'Amministratore deve provvedere ad adempiere a quanto prescritto dal Provvedimento del Garante per la protezione dei dati personali l'8/04/2010.**

Relativamente ai **Responsabili esterni**, l'ente ha ritenuto di **confermare la nomina di**:

- **GEA S.r.l** (P.IVA 03764380261) e **Consulenti Associati** (c.f. e P.IVA 03690390269), con sede entrambi in Preganziol (TV) Via Terraglio 397, in qualità di responsabili esterni rispettivamente per l'elaborazione delle retribuzioni/compensi dei propri dipendenti/collaboratori e per la consulenza del lavoro, legale, fiscale, e per tutti gli adempimenti connessi in materia previdenziale, assistenziale e del lavoro.

  Nell'ambito del rapporto contrattuale e dell'incarico professionale conferito, il Titolare trasmette allo Studio ed alla Società, oltre che dati personali comuni, anche i dati sensibili dei propri dipendenti in adempimento di obblighi di legge e di contratto (ad esempio, la trattenuta sindacale nel cedolino paga, dati relativi ad infortuni, maternità, etc.).

I Responsabili sopra individuati sono già stati nominati, previa deliberazione della Deputazione Amministrativa n. 342 del 3 Dicembre 2004.

Il Consorzio nomina **GEOS S.r.l.**, con sede in Pistoia (PT) Via Landucci 33, avente l'incarico di Responsabile del Servizio di Prevenzione e Protezione dei rischi sul lavoro ai sensi del DLgs n. 626/1994, responsabile esterno limitatamente al trattamento dei dati personali e sensibili necessari per l'adempimento dell'incarico stesso.

Si rileva inoltre che tra i soggetti che accedono ai dati del Consorzio figura il Medico del Lavoro, il **Dott. Luigi Rossi**, con studio in Capannori (LU) Via dei Babbi 28. Lo stesso tratta dati personali e sensibili in qualità di titolare autonomo del trattamento e i relativi dati anche sanitari sono protetti nell'archivio sanitario sotto la sua responsabilità.

Si ricorda poi che il Codice sulla privacy definisce gli ***incaricati*** come le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (art. 4, comma 1, lett.h).

Nel Consorzio il trattamento dei dati personali viene effettuato solo da soggetti che hanno avuto un formale incarico mediante designazione per iscritto. Le lettere di incarico, con le quali si individua l'ambito del trattamento consentito e si danno istruzioni sulle modalità del trattamento, sono già allegate al presente documento e ne costituiscono parte integrante.

Tuttavia, considerato che il Disciplinare Tecnico prevede che l'individuazione dell'ambito del trattamento consentito ai singoli incaricati debba essere ***aggiornato con cadenza almeno annuale***, si è provveduto ad effettuare le nuove lettere di incarico redatte per classi omogenee, come era stato valutato nelle precedente edizione del DPS, **con la comunicazione della nomina dell'amministratore di sistema.**

Il Consorzio ha autorizzato gli accessi ed i relativi trattamenti in funzione delle attività svolte in ciascuna Area funzionale, delle mansioni affidate a ciascun incaricato ed in relazione alla necessità di accedere agli stessi dati (principio di necessità del trattamento).

A ciascun incaricato sono stati assegnati compiti dettagliati, specificando puntualmente l'ambito del trattamento consentito in merito all'organizzazione e alle procedure di trattamento dei dati personali, con particolare attenzione ai dati sensibili ed all'adozione delle misure idonee e minime di sicurezza.

Relativamente all'aggiornamento degli incaricati interni, si specifica che vi sono nuovi incaricati: dal 08/11/2010 Bonfanti Mattia, dal 10/03/2011 il Sig. Canigiani Francesco e Neri Lorenzo e che sono cessati il sig. Pucci Gabriele il 14/04/2010, il sig. Boschi Alfredo il 30/06/2010.

Si richiamano qui di seguito gli incaricati interni **aggiornati,** ordinati per aree omogenee, del **Consorzio di Bonifica del Padule di Fucecchio**:

N°	NOMINATIVO	QUALIFICA	AREA DI APPARTENZA	AMBITO DEL TRATTAMENTO (Natura dati)
1.	**Franco Fambrini**	Direttore Generale	**DIREZIONE GENERALE**	Trattamento dati personali, sensibili e giudiziari, in

				formato elettronico e cartaceo
2.	Riccardo Ferri	Quadro	SETTORE AMMINISTRATIVO	Trattamento dati personali, sensibili e giudiziari, in formato elettronico e cartaceo
3.	Massimo Anziiotti	Impiegato Collaboratore amministrativo	SETTORE AMMINISTRATIVO	Trattamento dati personali, sensibili e giudiziari, in formato elettronico e cartaceo
4.	Claudia Cecconi	Impiegato Collaboratore amministrativo	SETTORE AMMINISTRATIVO	Trattamento dati personali, sensibili e giudiziari, in formato elettronico e cartaceo
5.	Gabriele Giuntoli	Impiegato Collaboratore amministrativo	SETTORE AMMINISTRATIVO	Trattamento dati personali, sensibili e giudiziari,in formato elettronico e cartaceo
6.	Gino Niccolai	Impiegato Ausiliario d'ufficio	SETTORE AMMINISTRATIVO	Trattamento dati personali, in formato elettronico e cartaceo
7.	Gino Giulietti	Impiegato Collaboratore amministrativo	SETTORE CATASTO	Trattamento dati personali, in formato elettronico e cartaceo
8.	Paola Marchesini	Impiegato Collaboratore amministrativo	SETTORE CATASTO	Trattamento dati personali, in formato elettronico e cartaceo
9.	Molendi Federica	Impiegato Collaboratore amministrativo	SETTORE CATASTO	Trattamento dati personali, in formato elettronico e cartaceo
10.	Cristina Bartolini	Quadro	SETTORE CATASTO	Trattamento dati personali, in formato elettronico e cartaceo
11.	Guelfi Massimiliano	Impiegato Collaboratore amministrativo	SETTORE CATASTO	Trattamento dati personali, in formato elettronico e cartaceo
12.	Simona Cecili	Impiegato Collaboratore tecnico	SETTORE TECNICO/AMMINISTRATIVO	Trattamento dati personali, in formato elettronico e cartaceo
13.	Caterina Turchi	Impiegato Capo sezione Opere in concessione	SETTORE OPERE Sezione Opere in concessione	Trattamento dati personali, in formato elettronico e cartaceo
14.	Bonfanti Mattia (in sost. Caterina Turchi assente)	Impiegato Capo sezione Opere in concessione	SETTORE OPERE Sezione Opere in concessione	Trattamento dati personali, in formato elettronico e cartaceo
15.	Cristiano Nardini	Impiegato Collaboratore	SETTORE OPERE	Trattamento dati personali, in formato elettronico e

16.	Lorenzo Galardini	tecnico Quadro	SETTORE OPERE	cartaceo Trattamento dati personali, in formato elettronico e cartaceo
17.	Marco Cortopassi	Impiegato Collaboratore tecnico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
18.	Claudio Miniati	Quadro	SETTORE TECNICO/AMMINISTRATIVO	Trattamento dati personali, in formato elettronico e cartaceo
19.	Valerio Fontana	Impiegato Collaboratore tecnico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
20.	Roberto Battaglini	Impiegato Collaboratore tecnico	SETTORE TECNICO/AMMINISTRATIVO	Trattamento dati personali, in formato elettronico e cartaceo
21.	Aldo Stefano Guggino	Impiegato Collaboratore tecnico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
22.	Vittorugo Franchi	Impiegato Applicato Amm. Guardiano idraulico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
23.	Matteo Bertellotti	Impiegato Applicato Amm. Guardiano idraulico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
24.	Riccardo Sorini	Impiegato Applicato Amm. Guardiano idraulico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
25.	Di Piazza Massimo	Impiegato Collaboratore tecnico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
26.	Chiostri Edoardo	Collaboratore tecnico direttivo	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
27.	Cappelli Luca	Applicato amministrativo – Guardiano idraulico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
28.	Neri Lorenzo	Applicato amministrativo – Guardiano idraulico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo
29.	Canigiani Francesco	Applicato amministrativo – Guardiano idraulico	SETTORE OPERE	Trattamento dati personali, in formato elettronico e cartaceo

Come **custode delle copie delle credenziali viene confermato il *Dott. Riccardo Ferri***, sopra individuato, persona cui spetta la custodia delle copie delle parole chiave (passwords) per accedere agli strumenti elettronici dell'Amministratore di sistema, detenute in busta chiusa, all'interno della cassaforte chiusa a chiave presso l'Ufficio Amministrativo.

Il ruolo riconosciuto al custode delle copie delle credenziali è previsto dal punto 10 del Disciplinare Tecnico il quale prevede che "quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato."

Ricollegandosi a quanto evidenziato sopra ed a completamento, nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal D. Lgs. 196/2003, all'esterno della struttura del Titolare, si adottano i criteri appena accennati (nomina responsabile), al fine di garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 D. Lgs. 196/2003 e dal disciplinare tecnico, allegato B al codice.

In linea generale, ai prestatori di servizi esterni che, in virtù di un contratto d'opera o di appalto trattano dati personali del Consorzio, è necessario richiedere un'apposita "dichiarazione di conformità", con la quale essi attestino di effettuare il trattamento dei dati personali ai quali sono autorizzati in conformità al d.lgs. n. 196/2003, ovvero predisporre apposite clausole contrattuali in tal senso.

Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario affinché quest'ultimo rispetti quanto prescritto per il trattamento dei dati personali.

Inoltre, se il titolare si avvale di soggetti esterni alla propria struttura per adottare misure minime di sicurezza, lo stesso deve farsi rilasciare dall'installatore (ad esempio, software house, consulente informatico), oltre che una descrizione scritta dell'intervento effettuato, anche una dichiarazione con la quale questi ne attesta la conformità alle disposizioni del disciplinare tecnico (Allegato B) al t.u. privacy).

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento sui dati personali contenuti negli strumenti

elettronici, salvo i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Relativamente agli addetti alla gestione e manutenzione del sistema informativo, sono confermati i seguenti nominativi:

ADDETTI ALLA GESTIONE E MANUTENZIONE DEL SISTEMA INFORMATIVO		
NOMINATIVO	**FINALITA'**	**TRATTAMENTO AUTORIZZATO**
ITALWAY S.R.L. Via Fucini nr. 2/B 51010 Massa e Cozzile (PT)	Assistenza e manutenzione Mail Server Exchange, gestore della connessione ADSL, manutentore della rete e dei sistemi di back up. Consulenza informatica su problematiche Terminal Server e SQL	Eventuale trattamento dei dati personali per attività di assistenza tecnica e consulenza (lettera 30/05/2005)
STR S.P.A. Via Gramsci nr. 36 46020 Pegognaga (MN)	Assistenza e manutenzione programma contabilità lavori e preventivazione (computo metrico) Settore tecnico	Eventuale trattamento dei dati personali per attività di assistenza tecnica (lettera 30/08/2005)
CAPACITAS S.R.L. Via Monte Popera nr 4/21 San Donà di Piave (VE)	Assistenza e manutenzione Software (GEPRO - Gestione protocollo; OPENCATASTO – Gestione Catasto)	Eventuale trattamento dei dati personali per attività di assistenza tecnica (lettera 30/08/2005)
GIACOMELLO STEFANO Via Marin Sanudo nr. 13/5 30020 Gaggio di Marcon (VE)	Assistenza e manutenzione programma contabilità finanziaria	Eventuale trattamento dei dati personali per attività di assistenza tecnica (lettera 30/08/2005)
E.T.G. SRL Via di Porto nr. 159 50018 Scandicci (FI)	Assistenza e manutenzione Sistema Videosorveglianza	Eventuale trattamento dei dati personali per attività di assistenza tecnica

Si evidenzia che possono accedere ai locali del Consorzio persone non autorizzate al trattamento dei dati personali (ad esempio, ditta di pulizie). A tali soggetti autorizzati esclusivamente all'accesso ai locali per lo svolgimento di determinate mansioni non è consentito in alcun caso il trattamento di dati personali, salvo casi eccezionali individuati puntualmente nella lettera di conferimento di incarico.

Allo stato attuale, gli addetti esterni autorizzati all'accesso ai locali sono i seguenti. Si specifica che è stata sostituita la Ditta di Pulizie, evidenziata in grassetto.

ELENCO ADDETTI ESTERNI AUTORIZZATI ALL'ACCESSO AI LOCALI		
NOMINATIVO	**FINALITA'**	**TRATTAMENTO AUTORIZZATO**
LA NUOVA SPLENDENTE **Via Benedetto Croce nr. 20**	**Pulizia locali**	**Nessuno, ad eccezione della distruzione dei documenti su supporto cartaceo gettati nei**

51011 Buggiano (PT) **C.f. e P.IVA 00932240476**		**cestini**
LUCARELLI S.R.L. Via P. Savi ncm 51016 Montecatini Terme (PT) C.f. e P.IVA 00321470478	Vigilanza dei locali	Nessuno (Lettera 26/03/2009)
SCRIPTA MANENT COOPERATIVA SERVIZI PER GLI ARCHIVI Via di Fabbrica nr. 1 51030 San Felice (PT) C.f. e P.IVA 01476410472	Riordino archivi consortili	Nessuno, ad eccezione della consultazione necessaria ai fini del riordino degli archivi (Lettera 10/03/2009)

3. Descrizione del Sistema Informatico del Consorzio

Il capitolo descrive gli elementi fondamentali del sistema informatico del Consorzio, con particolare riguardo alle misure di sicurezza previste al punto 19 del disciplinare tecnico allegato al d.lgs. n. 196/2003.

Come previsto dall'art. 3 del Codice in Materia di Protezione dei Dati Personali (D. Lgs. 30/06/03 n. 196), i sistemi ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

L'architettura informatica dell'ente è la seguente rimasta invariata rispetto al precedente aggiornamento.

N° e Tipo Server	N° Client	N° e Tipo Switch/Hub	N° e Tipo Router/Modem	N° e Tipo Collegamenti Wireless	Accessi Esterni	Altri Servizi
1 Primary Domain Server	25	Allied Telesyn AT-FS 724I (24 porte)	Zyxel 650H-E1	NO	VPN	NO
1 Server monitoraggio	3	3COM 10/100-16 PORTE (n. inv. 507)	n.2 MODEM GSM/GPRS		VNC	
1 Application Server SQL		D-Link DGS-1248T (44 porte)				
1 Primary Domain Server	26	D-Link DGS-1248T (1GBIT) (44 porte)				
1 Mail Server SBS						
1 Firewall Kerio						
1 PC Control Protection System						

Si individua qui di seguito l'**elenco dell'hardware**, indicando oltre che le caratteristiche dello stesso, l'incaricato che lo utilizza, le credenziali di accesso e la cadenza della modifica delle stesse, al fine di verificarne la conformità a quanto stabilito dal D.Lgs. n. 196/2003. L'ordine seguito è lo stesso utilizzato in precedenza per l'individuazione degli incaricati interni **aggiornato, con le modifiche evidenziate in grassetto.**

N° / Inventario	Hardware	Caratteristiche	S.O. Regolarm. licenziato	Software applicativi	Periferiche	Utilizzatore
1 499	PC Client IBM	Pentium Dual Core 2.2 Ghz 3GB Ram	Windows XP Professional	Software gestione centralino, Office XP	Stampante Hp Laserjet 1022	Sig. Fambrini
2 513	PC Client IBM	HP DC7900 SFF – INTEL CORE DUO 3.0 GHZ 3 GB RAM	Windows XP Professional		Lexmark C782 RETE, Hp Laserjet 4300 rete, **HP 2055DN**	Sig. Ferri
3 248	PC Client HP	HP Workstation Intel Core Duo Quad Core Q9300 2.5 Ghz 3GB RAM	Windows XP Professional	Software rilevazione presenze, software gestione variazioni mensili dipendenti e amministratori, Console gestione firewall Kerio, Suite adobe, Photoshop 7.0, Acrobat Professional 6.0, Pagemaker 7.0, Macromedia Freehand 11.0	Lexmark C782 RETE, Hp Laserjet 4300 rete	Sig. Anzilotti
4 514	PC Client IBM	HP DC 7900 SFF – INTEL CORE DUO 3.0 GHZ 3 GB. RAM	Windows XP Professional	Software gestione protocollo	Scanner Hp scanjet 8250, **Lexmark C782 rete, HP Laserjet 4300 rete**	Sig. ra Cecconi
5 313	PC Client IBM	P4 2.66GHz 512 MB. Ram	Windows XP Professional	Software gestione protocollo	Scanner Hp scanjet 8250, stampante Hp Laserjet 1015,	Sig. Giuntoli

					Lexmark C782 rete, HP Laserjet 4300 rete	
6 35	PC Client IBM	P4 2.66 GHz 512 MB. Ram	Windows XP Professional			Frontoffice/Niccolai
7 322	PC Client IBM	P4 2.66GHz 512 MB. Ram	Windows XP Professional	Software gestione protocollo	Stampante Hp **Office K550**, scanner Hp scanjet 5590	Sig. Giulietti
8 95	PC Client IBM	P4 2.66 GHz 512 MB. Ram	Windows XP Professional	Software gestione protocollo	Stampante Laserjet **2055DN,** scanner Hp scanjet 5590	Sig.ra Marchesini
9 491	PC Client IBM	P4 3.00GHz 512 MB. Ram	Windows XP Professional		Stampante Hp Laserjet **2055DN**	Sig. ra Molendi
10 488	PC Client IBM	P4 3.00GHz 512 MB. Ram	Windows XP Professional		Stampante Hp **Laserjet 2055DN**, Hp Laserjet 8100 rete	Sig. ra Bartolini
11 213	PC Client IBM	P4 2.66GHz 512 MB. Ram	Windows XP Professional		Stampante Hp Laserjet **8100**	Sig. Guelfi
12 59	PC Client IBM	P4 2.66GHz 512 GB. Ram	Windows XP Professional		Stampante Hp Business inkjet 1000	Sig.ra Cecili
13 363	PC Client IBM	P4 3.40 GHz 1 GB. Ram	Windows XP Professional	Software FLO – 2D	Stampante Hp Laserjet Color 5500 rete, **Lexmark E260DN**	Sig. ra Turchi
14 192	PC Client IBM	Xeon 2.80 GHz 1 GB. Ram	Windows XP Professional	Autocad 2008, Software FLO – 2D	Stampante Hp Laserjet Color 5500 rete, Plotter Hp T1200, **HP LASERJET 1320**	Sig. Nardini
15 138	PC Client IBM	HP WORKSTATIO N Z400 – INTEL XEON 2.66GHZ 16 GB. RAM	Windows 7 Professional 64 BIT	Autocad LT **2012** – H-EDILUS AZTEC – FLO – 2D Stampante HP Deskjet 6980	Stampante HP Deskjet 6980	Sig. Galardini
16	PC Client	P3 1.133 GHz	Windows XP	Autocad LT	Stampante	Sig. Cortopassi

148	IBM	256 MB. Ram	Professional	**2011**	Epson Stylus Color 880	
17 183	PC Client compatibile	AMD K7 700 MHz. 768 MB. Ram	Windows XP Professional		Stampante Epson Stylus Color 880	Sig. Miniati
18 170	PC Client IBM	P4 2.66GHz 512 MB. Ram	Windows XP Professional		Stampante Epson Stylus Color 880	Sig. Fontana
19 66	PC Client IBM	P4 2.66GHz **25** GB. Ram	Windows XP Professional	Software FLO – 2D	Stampante Hp CP 1700 rete	Sig. Battaglini
20 71	PC Client IBM	P4 2.66GHz 1 GB. Ram	Windows XP Professional	Arcview v.8.3, Software FLO – 2D	**Lexmark E260DN,** Scanner Epson GT 10.000 (n. inv. 77)	Sig. Chiostri
21 108	PC Client IBM	P4 2.66GHz 512 MB. Ram	Windows XP Professional		Stampante Hp Officejet Pro K550	Sig.ri Sorini, Neri e Canigiani e Cappelli (guardiani del Consorzio)
22 207	PC Client IBM	P4 2.66GHz 512 MB. Ram	Windows XP Professional		Stampante Hp Laserjet Color 5500 rete	Sig. Guggino
23 340	PC Client IBM	P4 2.66 GHz 512 MB. Ram	Windows XP Professional	Software monitoraggio Winnet 5.0		Monitoraggio
24 274	PC Client IBM	P4 2.80 GHz **1.5 GB Ram**	Windows XP Professional	Macromedia Freehand 11.0	Stampante Hp Inkjet 5550	Sig. Biondi
25 98	PC Client Compatibile	P4 2.00 GHz 528 MB. Ram	Windows XP Professional	Software monitoraggio Winnet 5.0, software VNC server	Stampante Olivetti Job-Jet P210	Monitoraggio
26 516	Notebook	HP 4510S-INTEL CORE T6570 2.1GHZ 4GB. RAM	Windows 7 Professional		Key wireless USB per presentazioni	Amministrativo
27 515	Notebook	HP 4510S-INTEL CORE T6570 2.1GHZ 4GB. RAM	Windows 7 Professional			Amministrativo Dott. Fambrini
28 270	Portatile PC Acer Travelmate	Pentium II 1.0 GHz. 64 MB. Ram	Windows 98 Contenente solo dati tecnici, non personali			Tecnico Progettazione
29 248	PC Client IBM	P4 2.66GHz 1 GB. Ram	Windows XP Professional		**Lexmark E260DN**	Sig. Di Piazza

30 500	PC Client ACER	ATHLON VERITON L410 X2 4400 Dual Core 2GB Ram	Windows XP Professional	PC CORRIDOIO (demo dei lavori eseguiti dal Consorzio)

Si riporta qui di seguito l'**elenco dei server consortili**, evidenziando accanto alla tipologia, le caratteristiche, il sistema operativo regolarmente licenziato e la localizzazione degli stessi, invariato rispetto all'aggiornamento precedente.

N° Inventario	Tipologia	Caratteristiche	S.O. Regolarmente licenziato	Software applicativi	Periferiche	Localizzazione
494	Primary Domain Server	Xeon 3.0GHz. 3 GB.Ram	Windows 2003 Server S.P.2	Microsoft SQL Server, Microsoft Office XP, Capacitas gest. Catasto, protocollo e inventario, STR Area Tecnica, Contabilità finanziaria	HD esterno per copie	Stanza archivio II° piano
292	Server Application SQL	P3 2.0 GHz. 2.6 GB. Ram	Windows 2000 Server S.P.4	Microsoft SQL Server	HD esterno per copie	Stanza archivio II° piano
360	Mail Server SBS	P4 2.66 GHz. 1 GB. Ram	Windows 2003 SBS			Stanza archivio II° piano
291	PC Firewall Kerio	Pentium D 3.0 GHz. 2 GB. Ram	Windows Server 2003 S.P.2	Kerio Winroute Firewall		Stanza archivio II° piano
501	Primary Domain Server (slave)	Fujitsu Server ECONEL 100 INTEL Core Duo 3Ghz 2GB Ram	Windows 2003 Server	//	//	Stanza server II° piano
509	Primary Domain Server Monitoraggio (slave)	HP PROLIANT SERVER RACK SLAVE MONITORAGGIO-MOD. DL120G5	Windows 2003 Server	Software monitoraggio Winnet 5.0 software VNC Server	Modem GSM/GPRS radio	Stanza server II° piano
510	Primary Domain Server Monitoraggio (master)	HP PROLIANT SERVER RACK MASTER MONITORAGGIO-MOD. DL120G5	Windows 2003 Server	Software monitoraggio Winnet 5.0 software VNC Server	Modem GSM/GPRS radio	Stanza server II° piano
511	Primary	HP PROLIANT	Windows	Software		Stanza server II°

	Domain Server SQL Monitoraggio	SERVER RACK WEB SERVER - SQL MONITORAGGIO-MOD. DL360G5	2003 Server	monitoraggio Winnet 5.0 software VNC Server		piano

Elenco dei tipi di connessioni internet ed accessi esterni

Tipo Connettività	Provider	Router - Modem	Client – Server Connessi
ADSL	Tin.it	Zyxel 650H-E1	Mail Server SBS – PC Firewall Kerio
GSM/GPRS		MODEM (n. inv. 503)	Master server monitoraggio
GSM/GPRS		MODEM (n. inv. 506)	Slave server monitoraggio
RADIO UHF		MODEM (n. inv. 504)	Master server monitoraggio
RADIO UHF		MODEM (n. inv. 505)	Slave server monitoraggio

POSTA ELETTRONICA	
Dominio	**Descrizione**
@paduledifucecchio.it	e-mail aziendale

Elenco Sistemi di Protezione Informatici

Sistema Protezione Informatico	Ultimo Aggiornamento
Kerio Winroute Firewall v. 7.0.1 build 1098	Patch 2 del 19 Marzo 2011
Norton Symantec Antivirus Enpoint Protection Vers. 11.0.5002.333	Aggiornamento giornaliero

4. L'Analisi dei rischi che incombono sui dati (punto 19.3 Disciplinare tecnico)

4.1. Metodologia di analisi e valutazione delle soglie di rischio

L'analisi dei rischi (punto 19.3 Disciplinare tecnico) è stata il punto di partenza delle attività di definizione ed attuazione della politica di sicurezza del Consorzio, riportata in sintesi nell'allegato e) al DPS edizione "0", nell'aggiornamento del DPS in edizione 1.1, 2.1, 3.1 e 4.1.

Per poter svolgere questa analisi sono state, nelle precedenti edizioni, esaminate sulla base delle informazioni fornite dal personale intervistato, le principali caratteristiche tecniche degli edifici e dei locali ove si trovano i documenti su supporto cartaceo e in cui sono situati gli strumenti elettronici con cui si effettuano i trattamenti dei dati.

Sono state, inoltre, analizzate le caratteristiche tecniche informatiche degli strumenti elettronici presenti all'interno della struttura dell'ente.

Lo stesso è stato fatto nella presente edizione 5.1, verificando se i rischi evidenziati in precedenza sono ancora presenti, e se il Consorzio si è adoperato al fine di ridurli.

L'obiettivo dell'analisi dei rischi è, da un lato, quello di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e, dall'altro, di avere una mappa delle contromisure di sicurezza da realizzare.

L'analisi dei rischi che incombono sui dati si articola, come nelle precedenti edizioni, nei seguenti moduli:

- Identificazione delle risorse da proteggere (par. 4.2);
- Individuazione ed analisi delle tipologie di rischio, distinte fondamentalmente in due specie (par. 4.3): rischi derivanti dalla mancata o inidonea osservanza delle misure di sicurezza idonee e preventive (art. 31) e rischi derivanti dalla mancata o inidonea osservanza delle misure di sicurezza minime (articoli 33 – 36);
- Individuazione dell'insieme delle contromisure da realizzare e definizione delle Politiche di Sicurezza (Parte II);
- Politica di formazione degli incaricati (Parte III).

L'analisi dei rischi è effettuata sulla base delle linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati (elaborate dal CNIPA).

La valutazione del livello di rischio è basata su considerazioni soggettive secondo una scala che individua tre soglie di rischio:
Tabella 1

Indice	Descrizione
Lieve (L)	Con questa soglia viene individuato un rischio molto basso che identifica una minaccia remota e comunque rapidamente reversibile od ovviabile.
Medio (M)	Con questa soglia viene individuato un rischio superiore al precedente che identifica una minaccia remota, ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale ipotesi è già consigliabile pensare ad accorgimenti per contenere il rischio, intensificando i controlli e la formazione-informazione del personale.
Grave (G)	Con questa soglia viene individuato un rischio che comporta conseguenze difficilmente reversibili, pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica, organizzativa) per abbattere il rischio e contenerlo a livelli accettabili.

4.2. Identificazione delle risorse da proteggere

Per analizzare e valutare in modo esaustivo i rischi che incombono sui dati, è di fondamentale importanza individuare gli elementi che rilevano ai fini della sicurezza, e che quindi vanno protetti, e i relativi fattori di rischio.

Nello svolgimento di tale fase sono stati presi in considerazione il fattore sia tecnologico sia umano, analizzando non solo le componenti singolarmente considerate, ma anche come queste interagiscono tra di loro sia fisicamente sia logicamente.

Le risorse individuate si possono suddividere in 5 categorie:

- **Luoghi fisici:** Sono stati analizzati i luoghi ove fisicamente si svolge il trattamento o si trovano i sistemi di elaborazione o si conservano i dati.
- **Risorse hardware:** Sono state esaminate le apparecchiature elettroniche che sono coinvolte nelle operazioni di trattamento. Tra queste hanno particolare rilievo:
  - Server;
  - personal computer;
  - elaboratori portatili.
- **Risorse dati:** Sono stati analizzati tutti gli archivi contenenti dati personali trattati con strumenti elettronici o su supporto cartaceo.
- **Risorse software:** Sono stati esaminati tutti i software applicativi mediante i quali vengono effettuati trattamenti automatizzati.
- **Risorse professionali:** Sono state analizzate la formazione e le istruzioni fornite agli incaricati in materia di sicurezza e di trattamento dei dati personali.

4.3. Individuazione delle tipologie di rischio

I rischi che sono stati presi in considerazione sono fondamentalmente di due tipologie:

1. quelli che si riferiscono alla mancata adozione o non corretta applicazione delle "**misure idonee e preventive**" previste dall'art. 31 d.lgs. 196/2003;
2. quelli che concernono più in generale i rischi di sistema, ossia quelli relativi ai vari sistemi operativi informatici, ai programmi e procedure varie. Tali rischi sono conseguenti alla mancata predisposizione o non corretto utilizzo delle "**misure minime**", previste dal d.lgs n. 196/2003 (articoli 33 - 36) e dal Disciplinare tecnico in materia di misure di sicurezza.

L'analisi dei rischi è quindi articolata in due parti.

Una **prima parte** che identifica, valuta e contrasta i rischi indicati specificatamente dal decreto in oggetto, e cioè:

- il rischio di distruzione o perdita, anche accidentale, dei dati stessi;

- il rischio di accesso non autorizzato;
- il rischio di trattamento non consentito o non conforme alle finalità della raccolta.

Una **seconda parte** che riporta l'analisi dei rischi non individuati specificatamente, e che derivano dalla mancata o inidonea adozione delle misure minime di sicurezza (articoli 33 – 36).

4.3.1 PRIMA PARTE: rischi derivanti dall'inosservanza delle misure idonee e preventive (Art. 31)

Di seguito è riportata l'identificazione dei rischi individuati dall'articolo 31 del d.lgs n. 196/2003.

Rischio di distruzione o perdita, anche accidentale, dei dati

Per ridurre questo rischio si deve garantire:

- la DISPONIBILITÀ del dato, impedendo che i dati e le risorse siano resi irreperibili da persone mediante processi non autorizzati o da eventi accidentali;
- l'INTEGRITÀ del dato, che deve essere quello originario o legittimamente modificato, in relazione alla relativa facilità di procedure fraudolente capaci di apportare modifiche senza lasciare indizi.

I rischi derivanti dal trattamento informatico dei dati, elencati in ordine decrescente di importanza, sono i seguenti:

- virus informatici;
- errori umani dovuti a imperizia, negligenza o imprudenza;
- intrusione telematica nelle risorse da parte di personale non autorizzato;
- deterioramento nel tempo, inaffidabilità del mezzo fisico, malfunzionamenti hardware o software;
- eventi fortuiti o calamitosi (es.: incendi, allagamenti, etc.).

Il rischio maggiore è legato al danneggiamento o alla distruzione dei dati ad opera dei virus informatici che, grazie alle reti telematiche, sono sempre più diffusi e difficili da identificare.

L'errore umano è un rischio da non sottovalutare che deve essere ridotto attraverso la formazione obbligatoria (si veda il punto 19.6 del Disciplinare tecnico).

L'intrusione telematica nelle risorse che contengono dati personali è una componente di rischio non trascurabile in quanto nessun sistema di protezione è, o può essere, totalmente sicuro.

Il deterioramento nel tempo e gli eventi fortuiti o calamitosi, pur potendo avere effetti anche disastrosi, sono molto rari e di conseguenza il rischio ad essi collegato si può considerare minore.

I rischi derivanti dal trattamento su supporto cartaceo dei dati, elencati in ordine decrescente di importanza, sono i seguenti:

- intrusione fisica nei locali del consorzio o eventi dolosi;
- errori umani dovuti ad imperizia, negligenza o imprudenza;
- eventi fortuiti o calamitosi (es.: incendi, allagamenti, etc.).

Il rischio di intrusione per furto, duplicazione dei dati, diffusione a scopo di lucro o danneggiamento, è quello più rilevante.

L'errore umano, considerata anche l'assenza di un controllo di tipo informatico, è una componente di rischio non trascurabile.

Per gli eventi fortuiti o calamitosi vale quanto precedentemente espresso nel caso del supporto informatico.

Rischio di accesso non autorizzato ai dati

In questo caso si parla di "confidenzialità" del dato, nel senso che un determinato dato deve essere accessibile solo a chi è autorizzato.

Per ridurre questa tipologia di rischio, si deve disporre di una funzione di controllo degli accessi che copra l'intero sistema informativo e non solo le specifiche applicazioni.

I dati devono essere riservati (quindi accessibili solo da chi è autorizzato) ed autentici (deve esserci la garanzia e certificazione della loro provenienza).

I rischi derivanti dal trattamento informatico dei dati, elencati in ordine decrescente di importanza, sono i seguenti:

- accesso e modifiche non autorizzate del personale dipendente;
- intrusione fisica o telematica negli ambienti o sabotaggio;
- virus informatici.

Per quanto riguarda l'accesso ai dati, il rischio più rilevante è legato all'errore umano.

Il rischio legato alla pirateria informatica è sicuramente non trascurabile.

I virus informatici, generalmente progettati per la distruzione di dati, costituiscono un rischio minore.

I rischi derivanti dal trattamento su supporto cartaceo dei dati, elencati in ordine decrescente di importanza, sono i seguenti:

- errori umani dovuti a imperizia, negligenza o imprudenza;
- intrusione fisica negli ambienti o eventi dolosi.

Per l'accesso ai dati su supporto cartaceo, il rischio più rilevante è legato all'errore umano, mentre il rischio legato all'intrusione fisica negli ambienti o ad eventi dolosi è sicuramente non trascurabile.

Trattamento non consentito o non conforme alla finalità della raccolta

Per ridurre questa tipologia di rischio, si deve fare in modo che il trattamento definito per ogni banca dati rimanga tale e non possa essere modificato da nessuno, senza l'espressa volontà del titolare.

Al fine di ottenere tale risultato, è necessario agire soprattutto sull'organizzazione della Società, predisponendo un'idonea ed opportuna assegnazione delle responsabilità, nonché una gestione delle verifiche periodiche conforme al d.lgs. n. 196/2003, unitamente all'adozione di efficaci soluzioni tecniche.

Il rischio relativo al trattamento non consentito o non conforme alle finalità della raccolta rileva sia per i trattamenti di dati effettuati su supporto informatico sia per quelli effettuati su supporto cartaceo.

Alla base di tale tipologia di rischio vi è la mancata o insufficiente formazione ed informazione degli incaricati del trattamento dei dati.

4.3.2 SECONDA PARTE: individuazione dell'esposizione al rischio per la mancata o inidonea osservanza delle misure minime di sicurezza (Articoli 33-36 d.lgs. n. 196/2003)

Identificate le risorse da proteggere e tutelare al fine di trattare i dati personali in conformità al d.lgs. n. 196/2003, si devono ora esaminare le minacce e la vulnerabilità alle quali sono sottoposte le risorse stesse individuate nel par. 4.2.

Il verificarsi della violazione di uno degli elementi di rischio comporta, in qualsiasi caso, l'insorgere di perdite economico-finanziarie e l'aumento dei costi di gestione.

La valutazione dei rischi è realizzata, differentemente dalla edizione "0", e come nei successivi aggiornamenti, correlando la probabilità di accadimento (probabilità stimata) in funzione dell'entità dei possibili danni nel trattamento (rilevanza e gravità) e della pericolosità delle conseguenze (conseguenze).

La valutazione tiene conto in particolare del livello potenziale di danno, della frequenza e tipologia della perdita sottrazione o distruzione dei dati già accaduta, dell'esperienza lavorativa aziendale, dell'esposizione ai diversi rischi, dell'esperienza e formazione degli incaricati, delle misure di prevenzione e protezione adottate quali ad esempio dispositivi di protezione fisica e logica dei dati.

Attraverso il procedimento illustrato, si ottiene la valutazione del rischio connesso al trattamento da parte dell'incaricato.

Nelle seguenti tabelle è stata compiuta l'analisi dei rischi, avendo attenzione alla tipologia degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali, nonché all'impatto sulla sicurezza dei dati, in relazione a ciascun evento e alla gravità e probabilità stimata dell'evento stesso.

Per ciascun evento probabile di Rischio si sono individuate più avanti le contromisure adottate o da adottare (PARTE II).

EVENTI RELATIVI AL CONTESTO (Analisi dei rischi sui luoghi fisici)

VALUTAZIONE DEI RISCHI				
EVENTO			IMPATTO SULLA SICUREZZA	
Codice	**Rischio**	**Probabilità**	**Rilevanza e Gravità**	**Conseguenze**
R.F.1	Accessi non autorizzati a locali /reparti ad accesso ristretto.	Bassa	Alta	Duplicazione e diffusione a scopo di lucro e /o danneggiamento dell'immagine del Consorzio
R.F.2	Sottrazione di strumenti contenenti dati personali.	Bassa	Alta	Duplicazione e diffusione a scopo di lucro e /o danneggiamento dell'immagine del Consorzio Alterazione o distruzione di programmi e/o dati.
R.F.3	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, etc.), nonché dolosi, accidentali o dovuti ad incuria.	Bassa	Media	Alterazione o distruzione di programmi e/o dati. Perdita parziale o completa di programmi e/o dati. Impossibilità di utilizzo dei dati per determinati periodi di tempo.
R.F.4	Guasto ai sistemi complementari (impianto elettrico, climatizzazione..)	Media	Media	Perdita parziale o completa di programmi e/o dati. Impossibilità di utilizzo dei dati per

				periodi di tempo limitati.
R.F.5	Errori umani nella gestione della sicurezza fisica.	Media	Alta	Alterazione o distruzione di programmi e/o dati.

EVENTI RELATIVI AGLI STRUMENTI (Analisi dei rischi sui Dati e sulle risorse Hardware e Software)

VALUTAZIONE DEI RISCHI				
EVENTO			IMPATTO SULLA SICUREZZA	
Codice	**Rischio**	**Probabilità**	**Rilevanza e Gravità**	**Conseguenze**
R.S.1	Accessi esterni non autorizzati.	Bassa	Alta	Violazione privacy. Perdita parziale o completa di dati. Manomissione e alterazione dei dati.
R.S.2	Malfunzionamento indisponibilità o degrado degli strumenti.	Bassa	Alta	Alterazione o distruzione di programmi e/o dati. Perdita parziale o completa di dati.
R.S.3	Intercettazione di informazioni in rete.	Bassa	Alta	Perdita parziale o completa di programmi e/o dati. Impossibilità di utilizzo dei dati per periodi di tempo limitati.
R.S.4	Azioni di Virus informatici. o di programmi suscettibili di recare danno	Media	Alta	Perdita parziale o completa di programmi e/o dati. Impossibilità di utilizzo dei dati.
R.S.5	Spamming o tecniche di sabotaggio.	Bassa	Alta	Alterazione o distruzione di programmi e/o dati.

R.S.6	Impossibilità di ripristinare copie di backup.	Bassa	Alta	Perdita parziale o completa di dati.

COMPORTAMENTI DEGLI OPERATORI (Analisi dei rischi sulle risorse professionali)

VALUTAZIONE DEI RISCHI				
EVENTO			IMPATTO SULLA SICUREZZA	
Codice	**Rischio**	**Probabilità**	**Rilevanza e Gravità**	**Conseguenze**
R.P.1	Sottrazione di credenziali di autenticazione.	Bassa	Alta	Manomissione, alterazione e/o cancellazione delle basi dati connesse. Manomissione configurazioni.
R.P.2	Errore Materiale.	Media	Alta	Violazione Privacy. Perdita parziale o completa di dati. Manomissione e alterazione dei dati. Impossibilità utilizzo dati. Perdita del controllo del sistema.
R.P.3	Carenza di consapevolezza, disattenzione o incuria.	Media	Alta	Violazione Privacy. Perdita parziale o completa di dati. Manomissione e alterazione dei dati. Perdita del controllo del sistema.
R.P.4	Comportamenti sleali o fraudolenti.	Bassa	Alta	Violazione Privacy. Perdita parziale o completa di dati. Manomissione e alterazione dei dati. Perdita del controllo del sistema.

PARTE IIª
LE MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

1. Misure per garantire l'integrità e la disponibilità dei dati (punto 19.4 Disciplinare tecnico)

Lo sviluppo e l'approfondimento di questa seconda parte del Documento Programmatico sulla Sicurezza rappresenta la diretta conseguenza dell'attività di individuazione dei rischi svolta nella parte precedente.

Sono state individuate misure tali da garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità.

Dopo aver definito le misure necessarie, sono state esplicitate le modalità con le quali le misure minime di sicurezza vengono realizzate nella realtà organizzativa dell'ente, definite nel dettaglio nelle procedure allegate al presente documento.

Lo scopo della presente sezione è quello di evidenziare in quale maniera le misure minime di sicurezza richiamate dall'art. 33 del d.lgs. n. 196/2003 vengono effettivamente realizzate ed aggiornate in funzione delle nuove disposizioni dettate dal Codice sulla privacy, e tenuto conto dell'evoluzione dei sistemi informatici nella realtà tecnologica ed organizzativa del Consorzio.

In particolare, le disposizioni del Codice sulla privacy impongono di individuare, a seconda che il trattamento venga effettuato con strumenti elettronici o su supporto cartaceo, le seguenti misure minime di sicurezza:

Trattamenti con strumenti elettronici (art. 34)

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici (art. 35)

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

La Politica di Sicurezza si basa, dunque, sull'adozione delle misure di tipo fisico, logico ed organizzativo, sopra citate in forma sintetica, e descritte nel dettaglio più avanti e nelle procedure allegate al presente DPS.

La Politica di Sicurezza comprende aspetti legati alla:

- **Sicurezza fisica:** diretta a prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi IT, ed a proteggere le apparecchiature hardware da danni accidentali o intenzionali. Essa comprende, quindi, anche la sicurezza degli impianti di alimentazione e di condizionamento, la manutenzione dell'hardware e la protezione da manomissioni o furti;
- **Sicurezza logica:** diretta alla protezione dell'informazione e di conseguenza dei dati, applicazioni, sistemi e reti;
- **Sicurezza organizzativa:** diretta alla definizione dei ruoli, dei compiti, delle responsabilità e delle procedure per regolamentare gli aspetti organizzativi della Politica di Sicurezza.

Misure di sicurezza di tipo fisico adottate o da adottare

Codice Misura	Codice Rischio	Descrizione misura	Note ed indicazioni per la corretta applicazione
M.F.1	R.F.1	Custodia degli archivi cartacei in armadi chiusi a chiave. Misura da adottare **obbligatoriamente** in caso trattamento di dati sensibili.	Gli incaricati sono istruiti sulle modalità di custodia degli atti e documenti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative. Tutti i documenti su supporto cartaceo, contenenti dati personali sensibili e giudiziari, sono conservati in armadi chiusi a chiave nell'Ufficio Segreteria, Ragioneria e personale (Area Amministrativa). Gli incaricati al trattamento possono prelevare i documenti e atti necessari per lo svolgimento dei compiti loro affidati per il tempo strettamente necessario, controllandoli e custodendoli fino alla loro restituzione, in modo che ad essi non accedano persone prive di autorizzazione. Tali documenti e atti devono essere restituiti al termine delle operazioni loro affidate in modo che gli stessi rimangano custoditi negli armadi chiusi a chiave. Si precisa che l'incaricato deve, inoltre, garantire che i documenti e gli atti contenenti tali dati siano custoditi in un luogo chiuso a chiave nel periodo di eventuale temporanea assenza dalla postazione di lavoro. Si precisa che documenti amministrativi, tecnici e catastali sono conservati presso l'unità locale del Consorzio di Bonifica dove sono

			custoditi tali dati dalla costituzione del Consorzio fino all'anno 2005. Gli ultimi cinque anni sono conservati presso gli uffici consortili.
M.F.2	R.F.2	Custodia dei supporti magnetici in modo da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti	Come misura idonea di sicurezza, i supporti magnetici utilizzati per l'attività di backup (Full System) sono conservati in cassette di sicurezza presso la Tesoreria dell'ente.
M.F.3	R.F.3	Adozione di misure volte a prevenire ed a contenere il rischi di eventi distruttivi naturali ed artificiali, dolosi (Dispositivi antincendio; Dotazione di dispositivi antintrusione)	Considerata la posizione dell'ente, si esclude che, salvo eventi imprevedibili ed eccezionali, il rischio di perdita di dati a seguito di allagamento possa verificarsi. Al fine comunque di evitare danni da eventi di questo tipo, sono stati protetti i server situandoli in locali al II° piano. Gli archivi cartacei sono stati protetti custodendoli in posizioni riparate, utilizzando anche armadi ignifughi presso Settore amministrativo per i dati dei dipendenti. Per ciò che concerne la perdita di dati conseguente ad incendio, si precisa che sono state attuate le misure previste dalla legislazione in materia di prevenzione incendi. I locali della sede sono dotati di estintori per lo spegnimento dei focolai di incendio. L'ente ha comunque provveduto ad adottare le disposizioni di sicurezza stabilite dal D.Lgs. n. 626/1994 e il Consorzio si sta adeguando ai sensi del nuovo D. lgs 81/2008. Al fine di prevenire accessi non consentiti ai locali in cui vengono trattati i dati personali, il Consorzio ha dotato la struttura di: • sistema di allarme antintrusione attivo in ogni piano della sede consortile (sensore di movimento), quando gli uffici sono chiusi; • **sistema di allarme antincendio con rilevatore di fumi collegato al sistema di reperibilità del Consorzio: in caso di incendio viene allertato, tramite chiamata telefonica, il guardiano reperibile;** • **sistema di controllo della corrente elettrica: collegato al sistema di reperibilità del Consorzio: in caso di mancanza di corrente viene allertato, tramite chiamata telefonica, il guardiano reperibile;** • **portone con serratura blindata all'ingresso principale;** **A maggior tutela dei dati, verrà installato un sistema di allarme**

			collegato alla vigilanza che attualmente controlla la sede del Consorzio di Bonifica. **Nell'archivio consortile situato in Via Perosi, 14/16, a miglior tutela dei dati è stato installato un sistema di sicurezza antincendio.**
M.F.4	R.F.4	Continuità dell'alimentazione elettrica	I server e i pc sono collegati a gruppi di continuità che garantiscono una stabilizzazione dell'energia elettrica erogata. Tali gruppi garantiscono l'autonomia temporale necessaria ad avviare le corrette procedure di spegnimento dell'elaboratore, nell'ipotesi in cui si verifichi un'improvvisa assenza di energia. **Descrizione: APC Back UPS 650, Smart UPS 700, Smart UPS 1500, Smart UPS 750.**
M.F.5	R.F.5	Verifica della leggibilità dei supporti di backup	Periodicamente, i supporti di backup sono testati e verificati per accertare l'integrità dei dati registrati al fine di contenere i danni derivanti da errori umani nella gestione della sicurezza fisica.

Misure di sicurezza di tipo logico adottate o da adottare

Codice Misura	Codice rischio	Descrizione misura	Note ed indicazioni per la corretta applicazione
M.L.1	R.S.1	Sistemi di autenticazione ed autorizzazione.	Ad ogni incaricato, come credenziale di autenticazione, è stato assegnato un codice identificativo univoco (Username) che non potrà, neppure in futuro, essere associato ad altre persone, ed una parola chiave riservata (password). Agli incaricati sono state impartite le istruzioni per l'utilizzo e la successiva gestione della seguenti parole chiave: • Password per accesso alla rete; • Password specifiche per singoli applicativi; • Parola chiave dello screen saver del proprio PC. La password di protezione dello screen saver consentirà all'utente la disattivazione di quest'ultimo alla ripresa dell'attività. Tutti gli utenti che trattano dati sensibili hanno l'obbligo di dotare il proprio pc di questa password. • Parola chiave del BIOS per PC portatili. Le parole chiave sopra citate, assegnate inizialmente ***dall'Amministratore di sistema***, Sig. Anzilotti Massimo, sono state cambiate al primo accesso dagli incaricati. L'accesso al profilo degli utenti è consentito ***all'Amministratore di sistema***, la cui password è custodita in una busta sigillata dal

			responsabile del trattamento, che assolve il ruolo di custode delle credenziali. La parola chiave **deve** essere tenuta **segreta** e deve essere **modificata periodicamente** dall'incaricato (almeno ogni sei mesi per il trattamento dei dati personali comuni, tre mesi per il trattamento dei dati sensibili e giudiziari).
M.L.2	R.S.2	Aggiornamento software/hardware	**L'Amministratore di sistema** provvede ad aggiornare i sistemi operativi con cadenza almeno annuale, e semestrale per gli strumenti con i quali vengono trattati dati sensibili. Il Consorzio dispone di un collegamento ad Internet di tipo ADSL che permette, qualora i sistemi operativi siano opportunamente configurati, l'installazione regolare degli aggiornamenti emanati dalla casa produttrice dei sistemi operativi stessi. La manutenzione a livello software e hardware è affidata al **all'Amministratore di sistema** (cfr. PARTE I, punto 2).
M.L.3	R.S.3 R.S.5	Il Firewall (muro taglia-fuoco) è un sistema che, interposto tra la rete interna del Consorzio e l'esterno, si occupa di realizzare la politica di sicurezza e, controllando opportunamente i diritti di accesso, permette di limitare la bi-direzionalità del traffico informatico.	Il Firewall (Kerio) controlla tutto ciò che entra o esce dalla rete a cui è abbinato, usando una tecnica di ispezione denominata stateful inspection. Tale tecnica consiste nel comparare tutti i dati in transito con i profili di sicurezza predefiniti, per garantire che tutto ciò che transita attraverso i Firewall sia autorizzato. Il sistema consente di resistere agli attacchi esterni che cercano di penetrare la rete dell'ente (intrusioni informatiche, sabotaggio, intercettazioni) e fornisce un accesso remoto sicuro anche agli eventuali utenti del Consorzio e outsourcers che lavorano all'esterno dell'ente.
M.L.4	R.S.4	Predisposizione ed aggiornamento degli antivirus	Per ciò che concerne la perdita di dati o di danneggiamento degli stessi dovuta a virus, si precisa che tutti gli elaboratori in dotazione al Consorzio (PC E Server) sono stati protetti con programma antivirus di tipo client - server (Norton Symantec Antivirus **Enpoint Protection vers. 11.0.5002.333).** I "pattern " dei virus vengono aggiornati con schedulazione giornaliera. In tutti i casi, l'aggiornamento avviene in modo automatico.

			Il controllo antivirus dei dischi rigidi viene eseguito costantemente in automatico. Il programma antivirus è verificato con cadenza almeno semestrale. Il personale è stato adeguatamente informato sui comportamenti corretti da tenere per evitare di introdurre virus informatici all'interno dell'ente.
M.L.5	R.S.4	Definizione delle modalità con cui vengono gestite, nel Consorzio, internet e l'uso della casella di posta elettronica.	Tutti gli incaricati che ne hanno necessità in relazione alle loro mansioni ed attività sono autorizzati ad accedere ad Internet e sono dotati di casella di posta aziendale, previa autorizzazione del responsabile delle misure di sicurezza di carattere informatico. Sarà opportuno pianificare ed effettuare corsi di formazione sulle procedure operative da seguire, e sui possibili rischi connessi ad un utilizzo improprio di tali misure.
M.L.6	R.S.6	Definizione delle modalità di esecuzione e frequenza dell'effettuazione del salvataggio di copie dei dati e programmi	Sono stati individuati tutti gli archivi dei quali effettuare il backup periodico in base alla loro importanza, criticità e stabilità, prevedendo una **frequenza giornaliera** di salvataggio su HD interno ed esterno, a cura del responsabile delle misure di sicurezza di carattere informatico. Sono state fornite le istruzioni per consentire la ricostruzione dei dati e loro integrità ed accessibilità.

Misure di sicurezza di tipo organizzativo adottate o da adottare

Codice Misura	Codice rischio	Descrizione misura	Note ed indicazioni per la corretta applicazione
M.O.1	Tutti	Analisi dei rischi e Documento Programmatico sulla Sicurezza	Sulla base dell'analisi dei rischi è stato **aggiornato** il Documento Programmatico sulla Sicurezza. Questo documento sarà reso disponibile per la consultazione a tutti i responsabili ed amministratore di sistema e agli incaricati che ne facciano richiesta.
M.O.2	Tutti	Piano di verifica delle misure adottate	È stato stabilito un piano di verifica delle misure adottate. Tale piano è illustrato nell'allegato g) al presente DPS nella sezione "Piano di verifica delle misure adottate".

M.O.3	R.P.1 R.P.2 R.P.3	Piano di formazione degli incaricati ed identificazione degli incaricati preposti alle attività di trattamento	È stato predisposto un piano di formazione degli incaricati. Tale piano è illustrato nel presente DPS. Sono stati **nuovamente** individuati e nominati per iscritto gli incaricati preposti al trattamento, ai fini dell'**aggiornamento** dell'ambito del trattamento consentito agli stessi. A tali incaricati sono state impartite le istruzioni necessarie al fine di effettuare il trattamento dei dati in conformità al d.lgs. n. 196/2003, e sono state loro consegnate le **lettere di incarico aggiornate** dove sono indicate le norme operative e di sicurezza a cui attenersi alla luce delle novità introdotte dal testo unico in materia di privacy, **informandoli nella nomina dell'Amministratore di sistema.**
M.O.4	R.P.1 R.P.4	Assegnazione ed autorizzazione degli elaboratori su cui effettuare i trattamenti	Ad ogni incaricato è stato assegnato un elaboratore tramite il quale poter accedere agli archivi in formato elettronico, per poter effettuare i trattamenti a quali sia legittimato, come da censimento riportato nella Parte I^, punto 3.
M.O.5	R.P.1	Indicazione del custode delle copie delle credenziali di autenticazione.	È stato assegnato tale ruolo al responsabile del trattamento, ***Dott. Ferri Riccardo***, ed a lui spetta la custodia, in un luogo sicuro, della password dell'Amministrazione di sistema.
M.O.6	R.P.1 R.P.3	Indicazione dell'Amministratore di sistema	È stato nominato per iscritto l'Amministratore di sistema, ***Sig. Anzilotti Massimo,*** a cui è stato affidato il compito di sovrintendere alle risorse dei sistemi operativi degli elaboratori e dei data base, ai sensi del ***Provvedimento di carattere generale del Garante del 27 novembre 2008.***
M.O.7	R.P.4	Consegna del modello di clausola di "conformità" alle misure di sicurezza all'Azienda esterna che collabora nella gestione dei sistemi informativi.	È stato predisposto il modello di clausola di conformità alle misure di sicurezza previste dal D.Lgs. n. 196/2003 per le Società che collaborano nella gestione dei sistemi informativi. Le Società devono dichiarare che gli interventi effettuati sono conformi alle disposizioni dello stesso codice.

L'analisi che precede si basa su considerazioni di carattere soggettivo che l'organizzazione potrà approfondire nel corso del tempo, applicando una metodologia di analisi consolidata.

In particolare, gli **aspetti critici** emersi rimangono i seguenti:

- la possibilità per i singoli incaricati di disporre di supporti informatici rimovibili quali cd rom, dvd, dispositivi USB, che consentono copie non autorizzate dai dati e/o installazione di programmi non licenziati;
- la possibilità per i singoli incaricati di accedere liberamente ad internet;
- l'utilizzo di strumenti elettronici da parte di più utenti;
- mancata regolarizzazione di rapporti verso alcuni outsourcers in conformità al d.lgs. n. 196/2003, a causa della carenza di consapevolezza della normativa da parte degli outsourcers stessi;
- attività di verifica da organizzare in conformità alle frequenze stabilite dal d.lgs. n. 196/2003.

A completamento ed integrazione dell'analisi dei rischi e delle misure di sicurezza, e per consentire una più agevole consultazione del presente documento, segue la tabella riepilogativa dei rischi con l'indicazione delle relative contromisure adottate o da adottare.

Risorsa	Cod.rischio	Livello Rischio	Cod.Misure di Sicurezza adottate	Cod.Misure di Sicurezza da adottare
Cartacea	R.F.1	L	M.F.1 - M.F.2 -M.O.3 - M.O.4	
Informatica Cartacea	R.F.2	L	M.F.1 - M.F.2 - M.L.1	
Informatica Cartacea	R.F.3	L	M.F.1 - M.F.2 – M.F.3 – M.F.4 - M.O.4	
Informatica	R.F.4	M	M.F.4 - M.L.6 - M.O.4	M.O.2
Informatica	R.F.5	M	M.F.5 - M.O.4 - M.O.3	

Risorsa	Cod.rischio	Livello Rischio	Cod.Misure di Sicurezza adottate	Cod.Misure di Sicurezza da adottare
Informatica	R.S.1	L	M.F.1 – M.F.2 - M.F.3 – M.O.3 - M.L.1 - M.L.3	M.O.2
Informatica	R.S.2	L	M.F.4 – M.L.2	M.O.7
Informatica	R.S.3	L	M.L.3	
Informatica	R.S.4	M	M.F.4 - M.L.2 – M.L.4 M.O.3	M.O.2- M.L.5
Informatica	R.S.5	L	M.L.3	
Informatica	R.S.6	L	M.F.2 - M.F.4 - M.F.5 - M.L.6 - M.O.3	M.O.2

Risorsa	Cod.rischio	Livello Rischio	Cod.Misure di Sicurezza adottate	Cod.Misure di Sicurezza da adottare
Informatica	R.P.1	L	M.L.1 - M.O.4 - M.O.5 - M.O.3 - **M.O.6**	
Informatica Cartacea	R.P.2	M	M.F.2 - M.F.3 - M.F.4 – M.F.5 - - M.L.6 - M.O.3	M.O.2 - M.L.5.
Informatica Cartacea	R.P.3	M	M.F.2 - M.O.3 - **M.O.6**	M.O.2 -
Informatica Cartacea	R.P.4	L	M.F.2 - M.L.6 - M.O.3 - M.O.4 -	M.O.2 - M.O.7

2. Criteri per la protezione delle aree e dei locali (punto 19.4 Disciplinare tecnico)

Le misure che garantiscono la protezione delle aree e dei locali sono state individuate in funzione del layout del consorzio e sono state già descritte in parte nel paragrafo precedente nella sezione relativa alle misure di tipo fisico adottate.

Secondo quanto stabilito dal Testo Unico, si evidenziano qui di seguito le misure più opportune di cui si è dotato il **Consorzio di Bonifica del Padule di Fucecchio** per la protezione fisica dei server ed altri dati personali situati nei locali dell'ente:

- localizzazione e limitazioni all'accesso al locale server ai soli incaricati autorizzati;
- sistemi di chiusura dei locali/uffici ove sono custoditi i sistemi e/o archivi contenenti dati sensibili e giudiziari;
- custodia dei documenti cartacei e dei supporti di memorizzazione in scaffali o armadi chiusi a chiave;
- dispositivi antincendio;
- climatizzazione dei locali;
- custodia dei supporti di back up in cassette di sicurezza presso la tesoreria dell'ente;
- sistema di allarme antintrusione;
- sistema di allarme antincendio con rilevatore di fumi;
- sistema di allarme rilevatore della mancanza di corrente elettrica.

Le misure di sicurezza vanno adottate non solo in riferimento agli elaboratori presenti nel Consorzio, ma anche in riferimento ad altri strumenti elettronici (computer palmari, notebook, etc.) detenuti eventualmente a vario titolo da responsabili e/o incaricati sui quali transitano dati personali.

Le contromisure fisiche adottate si riferiscono alla individuazione di aree ad accesso controllato e selezionato, ai controlli fisici all'accesso, ai sistemi di chiusura dei locali, al possesso e gestione delle chiavi, alla sicurezza dei locali server contro il pericolo di danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti contenenti dati personali.

3. Criteri e modalità per assicurare l'integrità dei dati e la disponibilità in caso di distruzione o danneggiamento (punto 19.5 Disciplinare tecnico)

In questa sezione, sono stati definiti i criteri e le procedure per assicurare l'integrità e la disponibilità dei dati in caso di loro distruzione e/o danneggiamento.

Il disciplinare tecnico, infatti, impone l'adozione di procedure in grado di garantire il ripristino dei dati nel caso di danni a questi ultimi o alle strutture mediante le quali si procede al trattamento.

Per tali criteri si rinvia alla procedura 01, allegata al presente aggiornamento del DPS in edizione 4.1, nella quale sono specificati:

- Modalità di backup dei dati e loro conservazione:
  - Procedure per l'esecuzione dei backup;
  - Procedure per l'archiviazione dei backup;
  - Tipi e numero di copie dei backup eseguiti;
  - Utilizzo di casseforti od armadi per l'archiviazione dei supporti di backup;
  - Criteri di rotazione per il riutilizzo dei dispositivi e di eliminazione dei dispositivi obsoleti;
  - Procedure per la verifica della corretta registrazione dei backup;
  - Presenza di un responsabile per l'esecuzione e la verifica dei backup.
- Procedura per il ripristino dei dati:
  - Restore di copie di backup;
  - Piano di disaster recovery e/o business continuità;
  - Ulteriori accorgimenti tecnici per il salvataggio dei dati (sistemi dotati di mirroring, in RAID, di tipo hot-swap, dotati di alimentazione ridondante, sistemi in cluster).

4. Criteri per garantire l'adozione delle misure minime nel caso di trattamenti affidati all'esterno della struttura (punto 19.7 Disciplinare tecnico)

Il disciplinare tecnico impone di descrivere i criteri da adottare per garantire il rispetto delle misure minime nel caso in cui alcuni trattamenti (o parti di esso) siano effettuati all'esterno della struttura del titolare.

Al fine di garantire un adeguato trattamento dei dati è necessario che i soggetti esterni ai quali vengono affidati trattamenti di dati rilascino specifiche dichiarazioni o documenti, oppure assumano impegni anche su base contrattuale.

A tal fine il Consorzio può:

1. predisporre apposite clausole contrattuali/dichiarazioni di conformità mediante le quali concordare determinati comportamenti in materia di sicurezza nel trattamento dei dati;

2. nominare il soggetto esterno Responsabile esterno limitatamente ai trattamenti di competenza, come l'ente ha peraltro già fatto (cfr. parte I, punto 2).

Per un'analisi più approfondita si rinvia alla Parte I^, punto 2.

PARTE IIIª
FORMAZIONE ED ADEGUAMENTO DEL DOCUMENTO

1. Piani di formazione per gli incaricati del trattamento (punto 19.6 Disciplinare tecnico)

In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

Il Consorzio ha riconosciuto l'importanza della formazione delle risorse umane riguardo le tematiche della sicurezza, come elemento significativo di riduzione dei rischi al proprio sistema informativo e si è impegnato, nelle edizione "0" del DPS, a promuovere momenti formativi, in particolare al momento dell'ingresso in servizio o al momento di cambiamenti di mansioni di tali soggetti o all'introduzione di nuovi strumenti elettronici che hanno impatto sul trattamento dei dati personali.

A tal fine, ha già provveduto alla formazione dei propri incaricati organizzando un corso con un docente esterno esperto in materia di trattamento dei dati personali nel dicembre 2005, come peraltro risulta dall'attestato di partecipazione rilasciato dalla società che ha tenuto il corso stesso.

Relativamente agli incaricati impossibilitati a partecipare all'incontro formativo, il titolare ha provveduto, attraverso i propri responsabili interni, ad informarli ed istruirli sulle tematiche esposte durante il corso, consegnando loro la brochure informativa che riportava le slides spiegate durante l'incontro.

Quest'anno il titolare provvederà alla formazione dei nuovi incaricati con l'erogazione della formazione on line con attestato di valutazione finale e sarà cura del responsabile provvedere all'aggiornamento della formazione per gli altri incaricati, in occasione della consegna delle lettera di incarico aggiornate.

Gli adempimenti in termini di formazione nei confronti degli incaricati devono sempre essere quindi definiti in maniera specifica.

Gioca un ruolo essenziale, infatti, l'attenzione dell'operatore a ridurre i fattori di rischio, evitando comportamenti che possono recare danno, o comunque rendere meno sicura la protezione dei dati personali.

Si tratta, in generale, di avviare un processo di introduzione e diffusione della cultura della sicurezza nella gestione del dato personale, dell'importanza del suo trattamento ovvero, in senso stretto, di formazione finalizzata alla diffusione e conoscenza delle misure di sicurezza adottate nel consorzio.

E' opportuno **conservare tutta la documentazione** di cui l'ente si sia avvalso nell'attività di formazione e prevedere sistemi per registrare la partecipazione ai corsi, così da poter **provare l'avvenuta formazione degli incaricati.**

Il Disciplinare tecnico dispone che la formazione debba avere **carattere di periodicità** ed essere fornita in determinate occasioni (attribuzione dell'incarico, cambiamento del profilo di autorizzazione, introduzione di nuovi strumenti rilevanti rispetto al trattamento di dati personali).

Una corretta politica dei dati personali, così come delineata dal d.lgs. n. 196/2003, non può essere dissociata da un articolato programma di informazione e formazione, come espressamente indicato dal punto 19.6 del Disciplinare Tecnico, per rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati e delle misure per prevenire eventi dannosi.

Alla luce di ciò, l'ente ha quindi sviluppato linee guida e pianificato una formazione diretta a diffondere la cultura della sicurezza informatica e le politiche di gestione dei dati personali, organizzando quindi i corsi, anche con modalità e-learning a distanza, con valutazione finale.

2. Programma di revisione ed adeguamento del Documento Programmatico sulla Sicurezza

Il Documento Programmatico è inteso come un vero e proprio piano per la sicurezza, diretto ad avviare un processo di gestione del sistema privacy.

Il d.lgs. n. 196/2003 non si limita a descrivere e ad imporre le misure minime di sicurezza, ma obbliga anche il titolare ed i responsabili designati ad adottare gli opportuni strumenti e/o procedure per garantirne l'aggiornamento.

I controlli sull'efficacia delle misure previste nel documento avranno cadenza annuale.

Periodicità delle verifiche previste, dal disciplinare tecnico in materia di misure minime di sicurezza (cfr. piano di verifica):

Trattamento dei dati con l'ausilio di strumenti elettronici

MISURE DA VERIFICARE	DESCRIZIONE MISURA	TIPOLOGIA DEI DATI	CADENZA	ALL. B al D.Lgs. 196/2003 – Provv. 2008
Credenziali di autenticazione	Disattivazione in caso di mancato utilizzo dei medesimi per un periodo superiore ai 6 mesi.		6 mesi	7
Credenziali di autenticazione	Disattivazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.		sempre	8

Codice per l'identificazione	Una volta assegnato, non può essere assegnato ad altri incaricati.		sempre	6
Parola chiave	Per il trattamento di dati personali deve essere modificata ogni sei mesi.		6 mesi	5
Parola chiave	Per il trattamento di dati sensibili deve essere modificata ogni tre mesi.	Dati sensibili e giudiziari	3 mesi	5
Profili di autorizzazione	Possono essere individuati per singolo incaricato o per classi omogenee di incaricati.		sempre	13
Profili di autorizzazione	Verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.		1 anno	14
Lista degli incaricati autorizzati	Può essere redatta anche per classi omogenee di incarico.		1 anno	15
Antivirus	efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.		6 mesi	16
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici.		1 anno	17
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici.	Dati sensibili e giudiziari	6 mesi	17

Backup	Salvataggio dei dati con frequenza settimanale.		7 giorni	18
Ripristino accesso dati	Ripristino accesso dati in caso di danneggiamento degli stessi o degli strumenti elettronici.	Dati sensibili e giudiziari	massimo 7 giorni	23
DPS	Documento programmatico sulla sicurezza.		1 anno (entro 31/03)	19
Sistemi antintrusione	Protezione contro l'accesso abusivo nel caso di trattamento di dati sensibili.		sempre	20
Custodia dei supporti rimovibili di memorizzazione	Istruzioni organizzative e tecniche per la loro custodia e utilizzo.		sempre	21
Riutilizzo dei supporti di memorizzazione	Se non utilizzati devono essere distrutti o resi inutilizzabili, controllo sulla non recuperabilità delle informazioni precedentemente contenute.		sempre	22
Nomina amministratore di sistema	Lettera di nomina ai sensi del Provvedimento di carattere generale del Garante del 27 novembre 2008	Dati sensibili e giudiziari	Entro il 30 giugno 2009, prorogato al 15/12/2009	*Provvedimento di carattere generale del Garante del 27 novembre 2008* e *Comunicato stampa del 23 febbraio 2009*
Verifica attività amministratore di sistema	Controllo dell'operato dell'amministratore di sistema e la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti	Dati sensibili e giudiziari	Annuale	*Provvedimento di carattere generale del Garante del 27*

	dei dati personali previste dalle norme vigenti.			*novembre 2008*
Registrazione degli accessi dell'amministratore di sistema	Registrazioni *access log* devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità.	Dati sensibili e giudiziari	6 mesi	*Provvedimento di carattere generale del Garante del 27 novembre 2008*

Trattamento senza l'ausilio di strumenti elettronici

MISURE DA VERIFICARE	DESCRIZIONE MISURA	TIPOLOGIA DEI DATI	CADENZA	ALL. B al D.Lgs. 196/2003
Istruzioni scritte	Finalizzate al controllo e custodia dei documenti.		sempre	27
Profili di autorizzazione	Individuazione dell'ambito del trattamento consentito agli incaricati, individuati anche per classi omogenee.		1 anno	27
Procedure di controllo e custodia	Al fine di non consentire l'accesso a persone prive di autorizzazione.	Dati sensibili e giudiziari	sempre	28
Accesso controllato agli archivi	Le persone ammesse dopo l'orario di chiusura devono essere identificate e registrate.	Dati sensibili e giudiziari	sempre	29
Autorizzazione preventiva all'accesso	qualora gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di incaricati alla vigilanza.	Dati sensibili e giudiziari	sempre	29

3. Dichiarazioni d'impegno e firma

Il presente documento, redatto nel mese di **Marzo 2011**, viene firmato in calce da:

- *Sig. Biondi Gino,* in qualità di Commissario Straordinario del **Consorzio di Bonifica del Padule di Fucecchio.**

Esso verrà sottoposto per l'approvazione alla Deputazione, e successivamente allegato alla delibera.

L'originale del presente documento viene custodito presso la sede del Consorzio, per essere esibito in caso di controlli.

Una sua copia verrà consegnata:

- a chiunque, in qualità di responsabile e/o incaricato, ne faccia richiesta.

Nella relazione accompagnatoria del bilancio si riferisce dell'avvenuto aggiornamento del Documento programmatico sulla sicurezza.

Ponte Buggianese, 31 / 03 / 2011

Timbro e Firma del legale rappresentante

Consorzio di Bonifica Padule di Fucecchio

DELIBERAZIONE n. **53** del **20 APRILE 2011**

GARA D'APPALTO DEI LAVORI DI "MANUTENZIONE ORDINARIA PER L'ANNO 2011 DEGLI IMPIANTI CONSORTILI" - AGGIUDICAZIONE –

IL COMMISSARIO STRAORDINARIO

PREMESSO:

CHE con deliberazione commissariale n°13 del 9 Febbraio 2011 è stato approvato il progetto esecutivo relativo ai lavori di "Manutenzione ordinaria per l'anno 2011 degli impianti consortili";

- CHE il Consorzio di Bonifica del Padule di Fucecchio, in ottemperanza a quanto disposto dalla deliberazione di cui sopra ed ai sensi del vigente Regolamento per l'acquisizione di lavori, servizi e forniture in economia, ha indetto la gara con procedura negoziata mediante il criterio del prezzo più basso per l'aggiudicazione dei lavori in narrativa;
- CHE in data 19 Aprile 2011 in una sala del Consorzio di Bonifica del Padule di Fucecchio, si è proceduto all'aggiudicazione provvisoria della gara d'appalto dei lavori di "Manutenzione ordinaria per l'anno 2011 degli impianti consortili";

VISTO il verbale di gara che si può riassumere come di seguito riportato:

"Manutenzione ordinaria per l'anno 2011 degli impianti consortili"	
Importo dei lavori	**€ 27.016,80**
Numero di imprese partecipanti alla gara:	3
Numero di imprese ammesse alla gara:	3
IMPRESA AGGIUDICATARIA:	**Ditta Quadrini Vitale** Fauglia (PI)
Ribasso offerto	14,89%
IMPRESA SECONDA CLASSIFICATA:	**Edil B s.r.l.** Cerreto Guidi (FI)
Ribasso offerto	14,05%
Importo contrattuale	**€ 23.312,10**

Sede: 51019 PONTE BUGGIANESE (Pistoia) - Via Libertà, 28 - Tel. 0572/93221 - Fax 0572/634527
Web: www.paduledifucecchio.it e-mail: info@paduledifucecchio.it

VISTA la proposta di deliberazione presentata in data 20 aprile 2011 dal Responsabile del Settore "Tecnico-Amministrativo" Arch. Claudio Miniati;

VISTO il parere di legittimità presentato in data 20 aprile 2011 dal Direttore Generale del Consorzio Dott. Franco Fambrini;

RITENUTA la regolarità degli atti;

D E L I B E R A

APPROVARE il verbale della gara d'appalto indicato in narrativa, procedendo alle verifiche sul possesso dei requisiti prescritti dalla normativa vigente sulle ditte aggiudicataria e seconda classificata;

DARE ATTO che, una volta concluse a buon fine le operazioni di verifica di cui sopra, l'aggiudicazione diverrà efficace.

IL COMMISSARIO STRAORDINARIO
(Rag. Gino Biondi)