Consorzio Universitario della Provincia di Palermo

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dallo Consorzio Universitario della Provincia di Palermo, per comodità di seguito "Consorzio".
Il presente documento è stato redatto da _____ in qualità di _____, che provvede a firmarlo in calce.

Elenco dei trattamenti di dati personali

Il Consorzio tratta i seguenti dati:
dati comuni dei Docenti, Studenti, Ricercatori, Professionisti , dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali;
dati comuni del personale dipendente distaccato presso il Consorzio, strettamente necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria; mentre permarranno di esclusiva pertinenza dell'ente distaccante i trattamenti dei dati sensibili dello stesso personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o l'adesione ad organizzazioni sindacali;
dati comuni di Studenti, Ricercatori, Docenti, Professionisti, Tecnici o altri dagli stessi forniti per l'espletamento degli incarichi affidati al/dal Consorzio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
dati comuni di terzi, forniti dagli utenti per l'espletamento degli incarichi affidati al/dal Consorzio, compresi i dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari;
dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti i fini fiscali o dati di natura bancaria;
dati comuni di altri professionisti cui il Consorzio affida incarichi o si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti a finalità fiscali o dati di natura bancaria;
dati sensibili degli utenti, dagli stessi forniti per l'espletamento degli incarichi affidati al Consorzio, idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico;
dati sensibili dei clienti, dagli stessi forniti o acquisiti per l'espletamento degli incarichi affidati al Consorzio, idonei a rivelare lo stato di salute;
dati sensibili di terzi, forniti dai clienti o acquisiti per l'espletamento degli incarichi affidati al Consorzio, idonei a rivelare lo stato di salute;

dati sensibili di clienti o terzi, comunque afferenti la vita sessuale.

dati non pubblici vengono acquisiti previa l'informativa che si allega al presente D.P.S.
Questi dati vengono trattati e conservati in fascicoli riposti in schedari dotati di chiusura, nonché trattati tramite computer in rete, in locali protetti e con accesso ad internet, archiviati al termine della pratica.

La sede del Consorzio, presso la quale vengono trattati i dati, è ubicato in Via Maqueda, 100, piano terra; è dotata di portone di ingresso a chiusura automatica e con citofono, sorveglianza notturna, e porte sbarrate. I locali, che lo compongono, sono dotati di porta con chiusura a chiave, così anche l'archivio. La segreteria è ubicata in un locale separato dalla sala di attesa per i visitatori. Il Consorzio è dotato di armadio-cassaforte con chiusura a chiave.
Ogni locale è dotato di computer in rete, connesso ad internet con connessione ADSL sotto rete intranet, la cui regolamentazione e monitoraggio degli accessi, sottoposta alle vigenti normative di sicurezza e ordine pubblico è sottoposta e rimane di pertinenza dell'Amministratore di rete della Provincia Regionale di Palermo, presso la cui sede il Consorzio è ospite, farà eccezione l'eventuale disponibilità di computer in rete, con connessione ADSL ad internet per la ricerca sul web e i servizi di posta elettronica da destinare a fruitori esterni all'organizzazione, quali: stagisti, visitatori altri esterni che a qualsiasi titolo siano autorizzati ad avvalersi del servizio;
nel locale, ove è ubicata la segreteria si trova una postazioni di lavoro con computer con connessione ADSL ad internet .
Inoltre in questo locale e nel locale antistante si trovano le stampanti, il fax, la fotocopiatrice e lo scanner posti in maniera da essere agevolmente vigilati dagli operatori . Le linee telefoniche sono passanti dal centralino della Provincia Regionale di Palermo, che resta responsabile per la tutela e il funzionamento delle stesse.
I sistemi operativi utilizzati sono Microsoft Windows XP/Vista e successivi dotati di regolare licenza, Linux: distribuzione Fedora, Ubuntu , altre distribuzioni sotto licenze libere GNU open source, Mac OSX- 9
Per le proprie attività istituzionali il Consorzio adopera Internet Explorer, Firefox Mozilla, Safari ultima versione.
Posta Elettronica pubblica, per le limitazioni imposte dall' Amministratore della rete della Provincia Regionale il Consorzio non adopera programmi di gestione mail tipo Outlook Express, per tanto si avvale dei servizi messi a disposizione dai Gestori internet, in prevalenza: Gmail di google..
Per la posta certificata (PEC) è stato acquistato un servizio di corrispondenza elettronica presso ARUBA Srl, che rimane responsabile per tutte le disposizioni di legge al servizio riferite.
Il Consorzio per le attività di Office adopera per a gestione
Il sistema Antivirus in uso sono AVG Free, AVIRA Free o analoghi gratuiti
Il Sistema di gestione del Firewall di rete è di competenza dell' Amministratore rete della Provincia Regionale di Palermo.

I livelli di responsabilità sono distribuiti secondo la seguente tabella **:**

RESPONSABILITÀ	**COGNOME E NOME**
Titolare del trattamento	
Responsabile del trattamento dei dati	
Responsabile della sicurezza informatica	
Amministratore della rete	
Custode delle password	
Incaricati del trattamento dei dati come da allegato 1	
Incaricato dell'assistenza e della manutenzione	

degli strumenti elettronici	

I dati comuni degli utenti, dei fornitori o di terzi, i dati comuni di altri esterni e professionisti cui il Consorzio affida incarichi o si rivolge per consulenze, i dati giudiziari ove eventualmente necessari per la gestione dei rapporti riferiti ai servizi, i dati giudiziari di terzi, i dati sensibili degli utenti o fruitori delle iniziative consortili e di terzi sono trattati, oltre che dal titolare, anche da tutti gli incaricati. I dati comuni del personale dipendente, i dati sensibili del personale dipendente distaccato rimangono di esclusiva gestione del distaccante con procedure e vincoli propri; i dati contabili per la gestione di salario accessorio rimborso o spese dei dipendenti distaccati ; i dati afferenti i pagamenti a favore di terzi fornitori, la contabilità e i rapporti bancari del Consorzio sono esclusivamente tenuti dai dipendenti:

Nome Cognome	**Incarico**	**Fascia**		

i quali si occupano della amministrazione. Questi dati sono in rete solo per la parte contabile, gestita su piattaforma ospite della Provincia Regionale di Palermo; la restante massa di dati non sono in rete ma si trovano solo sui computer dei dipendenti e relativi server direzionali autorizzati a trattarli.
E' stata compiuta l'analisi dei rischi che si può così sintetizzare: per i dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali), i dati comuni dei professionisti e consulenti (dagli stessi forniti per l'espletamento degli incarichi affidati dal/al Consorzio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi), i dati comuni di terzi (forniti a qualsiasi titolo per l'espletamento degli incarichi affidati dal / al Consorzio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari) i dati comuni dei fornitori (concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) i dati comuni di altri consulenti, amministratori, partner e professionisti cui il Consorzio affida incarichi (quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) ed i dati comuni degli utenti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali: il rischio legato alla loro gestione può definirsi basso/medio
Per i dati sensibili del personale dipendente, i dati giudiziari degli utenti, i dati giudiziari di terzi, i dati sensibili degli utenti (dagli stessi forniti per l'espletamento degli incarichi affidati dal / al Consorzio) i dati sensibili di terzi (forniti dai clienti per l'espletamento degli incarichi affidati dal / al Consorzio) il rischio legato alla loro gestione è da definirsi medio, eccezion fatta per i dati riguardanti le pratiche in cui sono contenuti dati idonei a rivelare lo stato di salute, o dati giudiziari di clienti o terzi e le pratiche, quali quelle in materia di diritto familiare, con dati idonei a rivelare la vita sessuale. Per questi ultimi dati il rischio collegato alla gestione può definirsi alto. Per i dati sensibili afferenti cause di stato il rischio di gestione può essere definito maggiormente elevato.
Postazioni di lavoro:
nr. 1 computer, DELL Precision PWS390 CPU core INTEL , connesso in rete ed a internet, indirizzo IP 172.16.1.12, nella segreteria utilizzato da Mammoliti Tommasa
nr. 1 computer, DELL Precision PWS390 CPU core INTEL , connesso in rete ed a internet, indirizzo IP 172.16.1.51, nell' ufficio amministrativo, utilizzato da Loredana Torre
nr. 1 computer, DELL Precision PWS390 CPU core INTEL , connesso in rete ed a internet, indirizzo IP 172.16.1.53, nell' ufficio amministrativo, utilizzato da Laura Zarcone,

nr. 1 computer, DELL Precision PWS390 CPU core INTEL , connesso in rete ed a internet, indirizzo IP 172.16.1.230, nell'ufficio del Presidente utilizzato da Prof. Giuseppe Frisella
nr. 1 computer, COMEX CPU core INTEL connesso in rete ed a internet IP 172.16.1.3, nell'ufficio del Direttore, utilizzato dall' Avv. Antonino Ticali
nr. 1 computer, assemblato Micromax CPU core INTEL, connesso in rete ed a internet, indirizzo IP 172.16.1.200, dotato di stampante multifunzione autonoma, nell' ufficio di contabilità utilizzato da rag. Giuseppe Carini
nr. 2 computer, DELL Precision PWS390 CPU core INTEL , connessi in rete ed a internet, indirizzo IP 172.16.1.54-55 nell' ufficio amministrativo-informatico utilizzati da Giuseppe Chiazza
Tutti i PC del Consorzio possono stampare sulla stampante di rete mutifunzione, Marca: Konika Minolta Ineo+ 220, indirizzo IP 172.16.1.23.

Per quanto riguarda gli strumenti elettronici, possono verificarsi malfunzionamenti, guasti, eventi naturali, alterazioni delle trasmissioni. Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori, virus, intercettazioni dei dati.
Per quanto riguarda le aree ed i locali: possono essere colpiti da eventi naturali o accessi di terzi non autorizzati.
Per ridurre i rischi sono state adottate le seguenti misure: Autenticazione informatica, tale misura è stata adottata dotando ciascun incaricato di una password di almeno 8 caratteri (o minore per le caratteristiche del sistema). Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né al Consorzio. La stessa viene autonomamente scelta dall'incaricato e dallo stesso custodita in una busta chiusa che viene consegnata al titolare del trattamento, il quale provvede a metterla nella cassaforte del Consorzio in un plico sigillato. Ogni tre mesi ciascun incaricato provvede a sostituire la propria password. Si è altresì disposto che le password vengano automaticamente disattivate dopo tre mesi di non utilizzo. Inoltre si è disposto che a tutti gli utilizzatori di strumenti elettronici non lascino incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è stato inserito lo screensaver automatico dopo 5 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
Si è inoltre disposto che essi verifichino la provenienza delle e-mail e non operino operazioni di sharing.
Essendo gli incaricati autorizzati a trattare la quasi totalità dei dati, e nell'eventualità comunque quelli sensibili e giudiziari, non si è provveduto a dare disposizioni in caso di prolungata assenza o impedimento dell'incaricato, eccezion fatta per i dati trattati in via esclusiva dal dipendente _____, che cura la contabilità, per il quale è stato indicato per iscritto il nominativo dell'incaricato della sostituzione.
Ogni singolo computer è dotato di dispositivo antivirus che viene aggiornato con funzione automatica quotidiana e con scansione giornaliera per ogni aggiornamento antivirus, e comunque settimanale.
Allo stato attuale non vi sono server direttamente trattati dal Consorzio, tuttavia è previsto, nella eventualità, di implementare il server di firewall.
Per ogni singolo computer è prevista la funzione di aggiornamento automatico del sistema fornito dalla Microsoft mediante lo strumento: windowsupdate.
Analogo sistema di aggiornamento automatico è previsto per l'antivirus. E' stata data istruzione che, qualora nessun aggiornamento del sistema fosse segnalato automaticamente per un periodo di mesi 6, si provveda comunque ad attivare la funzione di controllo per verificare l'esistenza o meno di detti aggiornamenti automatici.
Qualora si provvedesse in proprio, è disposto l'obbligo di provvedere ad un backup settimanale dei dati e dei sistemi installati sul server su cd rom o sicure unità di backup, i quali vengono conservati e chiusi in un armadio metallico rinforzato e con chiave di sicurezza, è data disposizione di verificare, effettuato il backup, la leggibilità del supporto e che una volta a settimana si proceda alla verifica a campione della leggibilità dei dati; custode di detti backup si provvederà con nomina del Direttore.

Si obbliga la disposizione che, effettuato un backup, venga distrutto il precedente.
Si obbliga la disposizione che, terminata la trattazione di una pratica, ogni relativo file, o dato, esistente sui computer, sia cancellato. Si è disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche. I fascicoli vanno conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti.
Le comunicazioni a mezzo posta, o a mezzo telefax, dovranno essere tempestivamente smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato e consegnato all'interessato.
Il locale destinato all'archivio dovrà essere chiuso a chiave. La/il dipendente è incaricata/o di controllare l'accesso all'archivio. Fuori dall'orario di lavoro l'accesso all'archivio è consentito previa registrazione. Si è data istruzione che il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia riposto negli appositi sacchi di plastica, dopo trattamento di appositi taglierine distruggi documenti, in dotazione ai responsabili del trattamento, e che detti sacchi siano chiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detto materiale sia giornalmente asportato.
Il rischio di accesso ai locali del Consorzio, può essere definito basso, atteso che l'ingresso allo stesso è controllato dai servizi di guardiania dell'ente ospite Provincia Regionale di Palermo, e che l'accesso ai locali del consorzio è dotato di porta a vetri chiusa a chiave.
Il rischio di accesso alle singole stanze può essere definito basso, atteso che le stesse sono dotate di porte con chiusura e l'ingresso di terzi estranei avviene solo previa accettazione e controllo.
Il rischio di accesso ai singoli strumenti da parte di persone non autorizzate può essere definito basso, essendo controllato l'accesso da parte di terzi ai locali del Consorzio; la zona di attesa degli utenti e visitatori è distanziata dagli strumenti ed essendo gli stessi utenti e visitatori controllabili dalla segreteria.
Le aree ed i locali potrebbero essere interessati da eventi naturali, quali incendi, allagamenti e corto circuiti, pur avendo il Consorzio provveduto ad adottare le disposizioni di sicurezza stabilite dalla L. 81/2008. Essendo l'impianto elettrico del consorzio, che è parte dell'impianto di rete elettrica della Provincia Regionale di Palermo la quale già nel suo piano di sicurezza ha dichiarato che ha dotato di dispositivi salvavita l'impianto in questione, il rischio può quindi definirsi basso. Per quanto riguarda gli strumenti elettronici, il rischio può essere definito basso, essendo state adottate delle misure di sicurezza, tendenti a ridurre il rischio gravante sui dati e derivante dalla gestione di detti strumenti.
Per quanto riguarda la documentazione cartacea, il rischio può essere definito basso, essendo l'archivio dotato di chiave, gli schedari chiusi, ed essendo state adottate le altre misure indicate, fatta eccezione ovviamente per gli eventi naturali.
I telefax inviati su carta chimica sono stati riprodotti su carta normale per evitarne il deterioramento.
Per quanto riguarda i supporti di memorizzazione, il rischio di deterioramento dei dati da essi portati può essere ritenuto basso, attesi i frequenti back up, ed il fatto che essi sono conservati in un cassetto chiuso a chiave, così come i dischi di installazione dei programmi software adottati. Non vi sono elaboratori non in rete, non vi sono elaboratori non in rete e connessi ad internet, per cui nessun giudizio di rischio deve essere dato su detti strumenti.
Atteso -infine- che gli incaricati al trattamento dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio afferente la riservatezza, o la distrazione, o l'incuria degli stessi, può essere definito basso.
Inoltre i dati comuni e sensibili, per gli affari trattati dal Consorzio ed il tipo di utenti che ad esso si rivolgono non paiono essere, come detto, di particolare interesse per terzi.
Si ritiene che verranno adottate le seguenti ulteriori misure.
Entro il termine del 30.06.2011 sarà installato sistema di firma elettronica per la trasmissione delle e-mail.
Sarà inoltre adottata ogni altra misura che dal tecnico della manutenzione venisse ritenuta utile e necessaria per migliorare la sicurezza degli strumenti elettronici.

Sarà installato inoltre gruppo di continuità per il server. Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici, si predisporrà entro il 30.06.2011 apposito piano di ripristino degli stessi, impartendosi comunque sin d'ora le seguenti istruzioni:
avvertire il titolare del trattamento dei dati e l'incaricato che ha in custodia il supporto di backup nonché i supporti ottici contenenti i vari software del Consorzio installati sugli strumenti elettronici;
ove in vigenza di garanzia rivolgersi immediatamente e chiedere l'intervento del tecnico manutentore della ditta fornitrice sollecitandone al più presto l'assistenza;
reinstallati i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nei supporti di backup;
provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
verrà dato incarico al tecnico manutentore di suggerire ogni altra misura;
in ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;
al fine di evitare eventi di perdita e di danneggiamento degli strumenti elettronici e dei datti in essi contenuti, si prevede che per due volte all'anno sia effettuata manutenzione in modo adeguato dal tecnico incaricato.
La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali.
Inoltre, essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile o giudiziaria. La formazione è fatta dal titolare del Consorzio.
Nel caso in cui il trattamento dei dati comuni personali, sensibili e/o giudiziari venga affidato a soggetti esterni, che li trattino con strumenti elettronici, per avere la garanzia che essi adottano le misure minime di sicurezza si esigerà dagli stessi una dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale attestino di aver adottato le misure minime previste dal disciplinare.
Alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei al Consorzio, viene dato incarico scritto con richiesta di specificazione dei nomativi delle persone che accedono ed espresso invito a limitarsi alle sole attività pertinenti alla prestazione per cui accedono. Si allegano oltre l'informativa, la lettera di istruzioni agli incaricati, la lettera alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei al Consorzio.

Il responsabile per la sicurezza

_____

- Palermo, lì _____

Il titolare

_____