Manuale sulle Misure di Sicurezza e Organizzative in ambito privacy FONDAZIONE WELFARE AMBROSIANO

Redatto da:	Responsabile Privacy area Segreteria Generale Anna Heidi Ceffa
Data creazione:	20.07.2015
Approvato da:	FWA – Fondazione Welfare Ambrosiano – con delibera del Consiglio di Gestione e Consiglio di Indirizzo del 01.10.2015.
Distribuzione:	Solo uso interno
Destinatari:	Dipendenti, collaboratori, volontari, stagisti, membri degli organi
Aggiornato il:	01/10/2017

Sommario

INTRODUZIONE E STUTTURA DEL DOCUMENTO

La struttura del presente Documento, redatto per descrivere le modalità di adozione delle misure di sicurezza minime previste dall'art. 34 D.lgs. 196/2003, di quelle idonee previste dall'art. 31 e delle eventuali misure di sicurezza necessarie in relazione a specifici trattamenti.
Il Documento redatto dal Responsabile per la protezione dei dati personali della Fondazione Welfare Ambrosiano (di seguito "FWA"), di seguito denominato "Referente Privacy" (Romano Guerinoni) ed approvato con delibera del CDI del 01/10/2015, risulta finalizzato alla corretta gestione e trattamento, in ambito organizzativo e tecnologico, del dato personale (comune e/o sensibile) effettuato presso la FWA
Per ogni approfondimento sulla metodologia interna adottata si rimanda alle specifiche policy interne adottate da FWA.

SCOPO E CAMPO DI APPLICAZIONE

Il presente Documento ha l'obiettivo di attestare la conformità delle misure organizzative e di sicurezza a quanto stabilito dal Codice in materia di protezione dei dati personali (D.lgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.lgs. n.196 del 30 giugno 2003), nonché fornire indicazioni relative alla produzione, gestione, conservazione e trasmissione delle informazioni aziendali con particolare attenzione a quelle di tipo elettronico che, per loro natura, risultano particolarmente critiche.
In questo Manuale sono altresì individuati i trattamenti, direttamente o attraverso collaborazioni esterne ovvero funzioni accentrate, effettuati da FWA, in quanto titolare (o, a seconda dei casi, co-titolare del trattamento), con l'indicazione della natura dei dati e della struttura (ufficio, funzione, etc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.
Si individuano i sistemi informativi impiegati, le precauzioni di tipo tecnologico per garantire la protezione degli strumenti elettronici e il personale coinvolto per tipologia per tutti i livelli prescritti, nonché i disciplinari cui sono assoggettati i vari soggetti coinvolti nei trattamenti.
I soggetti, a vario titolo, a cui il presente Documento fa riferimento sono:

- il **Titolare**: FWA in persona del suo legale rappresentante che, nel complesso, esercita un potere decisionale autonomo sulle finalità e modalità di trattamento dei dati personali, ivi compreso il profilo della sicurezza.

- i **Dipendenti**: dipendenti , collaboratori e stagisti di FWA. Pertanto, laddove, qui di seguito, sia utilizzato il termine "Dipendenti", quest'ultimo è comprensivo anche dei collaboratori e degli stagisti.

- i **Volontari**:le persone fisiche che erogano servizi di FWA c/o la rete di sportelli

- i **Destinatari:** Dipendenti, volontari e membri degli organi.

- gli **Interessati**: le persone fisiche cui si riferiscono i dati personali ai sensi dell'art. 4 del D.Lgs. 196/03.

- i **Responsabili**: i soggetti nominati tali dal Titolare ai sensi dell'art. 29 del D.lgs. 196/2003.

- gli **Incaricati:** i soggetti nominati tali dal Titolare o dal Responsabile di area ai sensi dell'art. 30 del D.lgs. 196/2003

- li **Amministratori di sistema:** figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione dati o di sue componenti. Vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi (Provvedimento del Garante per la protezione dei dati personali del 27 Novembre 2008).
  Tali soggetti per FWA. sono: Digicamere Scarl e MGA Computer Service SRL .

RIFERIMENTI NORMATIVI E DOCUMENTALI

Il presente Documento è stato redatto in conformità a quanto previsto dalla normativa nazionale in vigore ed in particolare in conformità a quanto statuito dall'art. 34 e dall'Allegato B del Decreto Legislativo n. 196/2003 "Codice in materia di protezione dei dati personali". Si riportano, di seguito, i principali riferimenti normativi e documenti interni.

NORMATIVA ITALIANA

- **Decreto Legislativo 30 giugno 2003, n. 196** e successivi provvedimenti emanati dal Garante per la protezione dei dati personali e Allegato B (Disciplinare Tecnico in materia di misure minime di sicurezza)

- **Decreto Legislativo 8 giugno 2001, n. 231,** recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni e integrazioni.

- **Provvedimenti dell'Autorità Garante per la protezione dei dati personali**

  - **Provvedimento del Garante Privacy del 27 novembre 2008** e successive modificazioni relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"
  - **Provvedimento del Garante Privacy del 13 ottobre 2008** "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali"

DOCUMENTI INTERNI

1) Organigramma privacy FWA
2) Nomine a incaricati, responsabili e amministratori di sistema (interni ed esterni)
3) Architettura client/server con policy di sicurezza informatiche adottate da FWA
4) Inventario sistemi FWA
5)Elenco Utenti FWA- Struttura file server policy – Elenco sportelli
6) Check list amministratori di sistema
7) Informativa ai Dipendenti

1. STRUTTURA ORGANIZZATIVA A SUPPORTO DELLA PRIVACY

La Fondazione Welfare Ambrosiano (di seguito denominata "FWA") è stata costituita dal Comune di Milano, Provincia di Milano, Camera di Commercio di Milano e le OO.SS. CGIL\CISL\UIL di Milano con lo scopo di offrire un sostegno alle persone e ai rispettivi nuclei familiari, che svolgano attività lavorativa e\o professionale nel Comune di Milano, che si sono venuti a trovare, anche per la crisi economica vigente, in situazioni lavorative o personali a rischio di esclusione sociale o povertà se non adeguatamente sostenute.
Molti dei servizi vengono erogati all'utenza attraverso una serie di Portali (alcuni dei quali gestiti da soggetti terzi), accessibili agli utenti ai seguenti nomi di dominio:
https://www.fwamilano.org
http://www.milanoabitare.org

FWA per erogare i suoi servizi all'utente e per la gestione delle attività di staff, si avvale di partner tecnologici (es. DigiCamere, MGA Service srl) e di una rete di sportelli nell'area metropolitana di Milano.
Nel presente Manuale e negli allegati è possibile verificare l'elenco completo dei soggetti terzi, la titolarità e i trattamenti sviluppati per i partner strategici che trattano dati personali di titolarità di FWA o che offrono servizi IT a supporto dei processi e per finalità correlate alla fornitura di servizi istituzionali di FWA.

Presso ogni funzione di FWA, le risorse, mediante "Responsabili" o "Incaricati" (ognuno nell'ambito dell'attività lavorativa), effettuano il trattamento di dati personali di rispettiva competenza attenendosi, scrupolosamente, alle istruzioni ricevute, alle singole policy aziendali adottate ed ogni altra ulteriore indicazione, anche verbale, fornita dal Responsabile per la protezione dei dati personali di area o per il

tramite dal Referente Privacy.

FWA oltre al trattamento dei dati personali di cui è titolare (in maniera autonoma), può eseguire trattamenti di dati personali di titolarità di terzi soggetti giuridici (in particolare del Comune di Milano, dell'Agenzia delle Entrate, dell'Agenzia del Territorio e della Regione Lombardia) con i quali vengono condivisi ed erogati servizi all'utenza (es. Agenzia Milano Abitare) per tali motivi, alle volte FWA può rivestire il ruolo di co-titolare di determinati trattamenti.
In tali casi FWA è tenuta ad adottare tutte le misure per garantire la sicurezza delle informazioni e dei dati trattati, con riferimento ai trattamenti di cui è contrattualmente responsabile, e in ogni caso nel rispetto di quanto previsto dal Codice Privacy.

In sintesi il trattamento sui dati, operato da FWA può essere schematizzato identificando e classificando l'ambito del trattamento dei dati personali nel modo seguente:

1. FWA tratta dati personali nell'ambito dei suoi processi interni aziendali (così come riportato nell'organigramma privacy FWA.), anche attraverso i siti web sopra indicati. I trattamenti sono effettuati interamente da FWA;
2. FWA tratta dati personali di titolarità di terzi soggetti giuridici conformemente a quanto previsto da accordi sottoscritti. In questi casi, i trattamenti sono effettuati da FWA in qualità di titolare autonomo o co-titolare, direttamente nei confronti dei soggetti interessati (utenti).

FWA per alcune delle attività prestate può avvalersi dell'attività (ulteriori) di fornitori esterni designati Responsabili in outsourcing del trattamento (gestione piattaforme informatiche, sito web, etc.), i quali, a loro volta, potrebbero aver bisogno di sub-appaltare determinati servizi (attività di manutenzione, hosting etc.). In tali casi, al fine di non contravvenire al principio in base al quale un responsabile non può nominare a sua volta un altro responsabile, il Responsabile nominato da FWA sottoscrive con i propri terzi fornitori (sub-appaltatori) un accordo scritto che impone a questi ultimi il rispetto degli stessi obblighi a cui il Responsabile si è vincolato in virtù della designazione ricevuta da FWA e concernente il rispetto delle misure di sicurezza e di riservatezza in ambito privacy.
In allegato l'organigramma privacy di FWA. (Vd. Allegato 1).

2. TRATTAMENTO DEI DATI PERSONALI DI FWA.

FWA tratta dati personali nell'ambito della propria attività istituzionale e promozionale dei servizi sopra indicati. I trattamenti sono eseguiti mediante operazioni elettroniche attraverso il sistema informativo di FWA ed i propri siti web o di piattaforme web gestite da terzi nonché mediante operazioni manuali e cartacee. Tali operazioni di trattamento sono eseguite da coloro che operano in qualità di Responsabili o Incaricati da FWA e da parte di soggetti esterni nominati dalla stessa Responsabili del trattamento in outsourcing o nella qualità di Titolari autonomi.

Struttura di riferimento: nel seguito è indicata la struttura (ufficio, funzione, etc.) all'interno della quale è effettuato il trattamento di dati personali di FWA, le Aree e gli Uffici, coordinati da persone espressamente nominate Responsabili dei relativi trattamenti di dati personali:

- **Area Microcredito**. Si occupa principalmente di evadere le richieste di microcredito (famiglia, impresa, Under 35) e inserite nella piattaforma dedicata, produrre le garanzie, tenere l'archivio cartaceo e digitale delle pratiche di microcredito, coordinare il processo operativo tra fondazione, sportelli della rete FWA, Banche convenzionate e Beneficiari dei servizi della Fondazione. (Responsabile art. 29 d.lgs. 196/2003 Anna Heidi Ceffa);
- **Area iniziative economiche nei quartieri della periferia milanese (Bandi Comune).** Si occupa principalmente di evadere i servizi ausiliari di accompagnamento alle imprese beneficiarie dei bandi del comune di Milano, indirizzati ad iniziative economiche nei quartieri della periferia milanese. . (Responsabile art. 29 d.lgs. 196/2003 Simonetta Chiodi);
- **Area Anticipazioni Sociali.** Si occupa principalmente della raccolta documentale e del caricamento in piattaforma delle richieste di CIGS/CIGD e dei contratti di solidarietà, fornisce la garanzia del prestito presso le banche convenzionate e gestisce il portale web dedicato alla raccolta e al controllo dei dati dei lavoratori e delle imprese richiedenti.(Responsabile art. 29 D.lgs. 196/2003 Alessandro Menarini);
- **Area Milano Abitare – Agenzia Sociale per la Locazione** si occupa principalmente di favorire l'incontro tra proprietari e inquilini disponibili a sottoscrivere un contratto di

affitto **a** canone concordato secondo gli accordi territoriali e offre ulteriori opportunità per i proprietari e gli inquilini che portano a termine l'accordo. (Responsabile art. 29 D.lgs. 196/2003 . Rosa Cioffi);
- **Area Segreteria Generale** si occupa principalmente delle attività di direzione e raccordo generale delle funzioni dei servizi offerti, nonché delle attività di coordinamento con le Funzioni Accentrate (Responsabile art. 29 D.lgs. 196/2003 Anna Heidi Ceffa);
- **Area amministrativa contabile** si occupa principalmente delle attività amministrative e contabili(Responsabile art. 29 D.lgs. 196/2003 Roberto Omegna - Colombo)

2.1. Strumentazione in generale

FWA procede al trattamento di dati personali comuni e sensibili. Tali dati sono trattati con l'ausilio di strumenti informatici. Per strumentazione si intende l'insieme di hardware e software messo a disposizione dei Dipendenti per le sole finalità lavorative.
Tale strumentazione dovrà essere utilizzata e conservata appropriatamente per preservarne l'integrità, la disponibilità e la riservatezza delle informazioni.
Rientrano nella definizione di strumentazione i personal computer (fissi o laptop), i telefoni cellulari, i tablet, gli smartphone messi a disposizione o utilizzati dal personale.
I software presenti in azienda sono gestiti da Digicamere, previa richiesta di FWA e secondo indicazioni fornite dalla stessa. Le postazioni dei PC, il server, il centralino sono gestiti da MGA Computer Service SRL che mantiene un elenco, da aggiornare con cadenza annuale, di tutte le attrezzature informatiche di cui si serve FWA per l'espletamento delle proprie attività, dello scopo cui sono destinate, della loro allocazione fisica, delle misure di sicurezza su di esse adottate e delle eventuali misure di adeguamento pianificate.

3. ELENCO DEI TRATTAMENTI

In questa sezione sono individuati i trattamenti effettuati, direttamente o attraverso condivisione esterna, da FWA., in quanto titolare (o co-titolare), con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

3.1. Natura dei dati trattati

Natura dei dati trattati: i dati trattati sono dati personali "comuni" e in taluni casi anche dati "sensibili", con riferimento - a titolo esemplificativo e non esaustivo - alla gestione ordinaria del rapporto di lavoro, alla gestione delle garanzie rilasciate per le pratiche di credito o di anticipazione sociale, alla gestione dei dati trattati per l'Agenzia Sociale per la locazione. La descrizione completa dei trattamenti interni e/o esterni e della natura dei dati effettuata da FWA. è riportata nell'Allegato 2 denominato "Catalogo dei trattamenti".
I trattamenti sono effettuati per le seguenti finalità:

- Organizzazione, promozione e la gestione dei servizi di garanzia del credito solidale, della CIGS/CIDG, dei servizi ausiliari al credito (accompagnamento, tutoring ecc..), dei servizi e delle agevolazioni previste per gli aderenti all'agenzia sociale per la locazione Milano abitare ;
- organizzazione e promozione di convegni, di commissioni di studio, di ricerche, corsi di formazione in materia di welfare sussidiario;
- adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi;
- esecuzione di specifici obblighi contrattuali;
- rilevazione del grado di soddisfazione dei beneficiari sulla qualità dei servizi resi e sull'attività svolta o per attività statistiche ad uso interno;
- elaborazione Buste paga / gestione Contratti di lavoro / Fatturazione dei servizi resi e finalità Amministrativo - Contabili.

FWA sulla base di una prima ricognizione, salvo apportare successive integrazioni o correzioni, dichiara di trattare i dati qui di seguito elencati:

- **a) dati comuni**
  Dato personale comune è da intendersi qualunque informazione relativa alla persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

- **b) dati sensibili**
  Dati sensibili sono quei 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Si elencano, nell'Allegato 2 "Catalogo Trattamenti", le categorie di dati che possono essere trattati e il relativo codice di trattamento in relazione a ciascuna funzione aziendale

3.2. Co-titolarità tra FWA, Comune di Milano, Agenzia delle Entrate (SISTER), Agenzia del Territorio (SIT), Regione Lombardia

Dall'apertura dell'Agenzia Sociale per la Locazione Milano Abitare(maggio 2015) ,FWA ha intrapreso un percorso finalizzato a massimizzare l'efficienza interna, attraverso l'accesso alle banche del Comune di Milano, dell' Agenzia delle Entrate (Sister)e e dell'Agenzia del Territorio (Sit), e l' integrazione dei dati. Tale intervento organizzativo, permette di gestire le risorse con maggiore flessibilità, di condividere le conoscenze e di incrementare la trasparenza, nonché di effettuare una lettura omogenea delle informazioni. Si tratta di attività che vengono svolte in maniera trasversale nei diversi enti coinvolti, valutati da team di lavoro "misti", ai fini di una corretta gestione e trattamento, in ambito organizzativo e tecnologico, del dato personale, per le quali è stato previsto uno specifico accordo di riservatezza per garantire l'adozione di specifici livelli di sicurezza ed evitare l'accesso ai dati da parte di soggetti non autorizzati.

3.3. Organi

Consiglio d'Indirizzo: composto da un numero minimo di cinque a un un massimo di quattordici membri. Verifica i risultati complessivi della gestione di FWA.

Consiglio di Gestione: composto da un numero minimo di quattro a un numero massimo di cinque membri. Provvede all'amministrazione, ordinaria e straordinaria, ed alla gestione della Fondazione.

Collegio Revisori: composto da tre membri effettivi nominati dal Consiglio d'indirizzo, è organo tecnico contabile della Fondazione, accerta la regolare tenuta delle scritture contabili, esamina le proposte di bilancio preventivo e di rendiconto economico finanziario ed effettua verifiche di cassa.

3.4. Trattamento dati affidati all'esterno

In questa sezione è esposto un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Per gli adempimenti di legge, per la gestione dei dati dei beneficiari o per altre attività di FWA . (es. manutenzione, hosting, newsletter), infatti, alcuni dati personali vengono affidati all'esterno e/o co-gestiti con altri titolari.

Alle società o soggetti a cui si affida l'incarico si richiede conformità di trattamento alle norme minime prescritte dal D. Lgs. 196/2003 e dall'Allegato B dello stesso.

Gli stessi, infatti, si sono impegnati, in qualità di Responsabile esterno al trattamento o di Titolare autonomo o co-titolare, nel trattamento dei dati degli Interessati a:

1. adempiere agli obblighi previsti dal Codice per la protezione dei dati personali, poiché i dati che tratterà nell'espletamento dell'incarico ricevuto sono comunque dati personali;

2. trattare i dati al solo fine dell'espletamento dell'incarico ricevuto;

3. rispettare le istruzioni specifiche contenute nella lettera di nomina, conformando ad esse le procedure già eventualmente in essere;

4. relazionare annualmente sulle misure adottate e di avvertire immediatamente i referenti della A.S. in caso di situazioni anomale o di emergenza;

5. riconoscere eventualmente il diritto di FWA. a verificare periodicamente l'applicazione delle norme di sicurezza adottate;

6. attestare l'adozione delle misure minime di sicurezza previste dall'art. 34 D.lgs. 196/2003 e del disciplinare tecnico Allegato B.

Pertanto, per le eventuali violazioni di legge poste in essere nell'ambito della propria attività di competenza, rispondono direttamente e in via esclusiva tali soggetti esterni.

Trattamenti affidati all'esterno Descrizione sintetica dell'attività esternalizzata	**Trattamenti di dati interessati**	**Soggetto esterno**	**Descrizione dei criteri e degli impegni assunti per l'adozione delle misure**
Servizio di amministrazione di sistema in outsourcing e di sicurezza ed assistenza informatica, realizzazione e gestione di pacchetti e strumenti informatici	Possibile accesso e visione a tutti i dati personali elettronici di titolarità di FWA	DigiCamere Scarl M MGA Computer Service srl	Designazione ad Amministratore di Sistema e Responsabile del trattamento in outsourcing ai sensi dell'art. 29 D.lgs. 196/2003, contenente specifica Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.
Gestione Data Center (servizio di hosting sistemi informativi) e delle piattaforme, di cui FWA. ha attivato il servizio on-line	Possibile accesso e visione a tutti i dati personali elettronici di titolarità di FWA	DigiCamere Scarl	Designazione a Responsabile del trattamento in outsourcing ai sensi dell'art. 29 D.lgs. 196/2003, contenente specifica Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.
Si occupa della gestione dei siti web www.fwamilano.org e www.milanoabitare.org (cura del layout) e fornisce il servizio di hosting; la stessa può avere accesso ai dati degli utenti beneficiari dei servizi di FWA	Possibile accesso e visione a tutti i dati personali elettronici di titolarità di FWA	DigiCamere Scarl	Designazione a Responsabile in outsourcing ai sensi dell'art. 29 D.lgs. 196/2003, relativamente alla gestione dei siti web e del blog, alle specifiche attività prestate e alle misure di sicurezza da implementare.

Si occupa de servizio di assistenza tecnica, gestione e manutenzione delle postazioni di lavoro hardware e software in dotazione presso FWA, nonché dello smaltimento	Possibile accesso e visione a tutti i dati personali elettronici di titolarità di FWA	MGA Computer Service srl	Ai sensi dell'art. 29 D.lgs. 196/2003, tale società è stata nominata Responsabile esterna del trattamento, con l'obbligo specifico di rilasciare in favore della A.S. l'attestato di conformità di cui alla regola 25 dell'Allegato "B" al Codice Privacy
Si occupa del servizio di accoglienza degli Interessati, del caricamento dei dati sulla piattaforma di proprietà di FWA	Possibilie accesso e visione ai dati personali elettronici e cartacei di pertinenza dei singoli profili e di titolarità di FWA	Sportelli FWA : ACLI -CGIL -CISL-UIL -FORMAPER-COOP LA STRADA -MICRO2 -AISTP -VOBIS	Designazione a Responsabile del trattamento in outsourcing ai sensi dell'art. 29 D.lgs. 196/2003, contenente specifica Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.
Servizio di amministrazione contabile e gestione del personale dipendente (contrattualistica, buste paga ecc…) di FWA	Possibile accesso e visione a tutti i dati personali dei dipendenti di titolarità di FWA	STUDIO TRIBERTI COLOMBO	Designazione a Responsabile del trattamento in outsourcing ai sensi dell'art. 29 D.lgs. 196/2003, contenente specifica Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.

3.5. Modalità di trattamento

I dati sopra elencati sono trattati in maniera elettronica, in forma prevalentemente automatizzata, e in forma cartacea, sia per quanto riguarda i dati personali di cui FWA è titolare sia per quanto attiene ai servizi resi in regime di co-titolarità.
Il trattamento dei dati avviene, quindi, mediante strumenti manuali, informatici e telematici (Server, File Server, posta elettronica, rete locale (LAN), rete periferica (WPN) rete internet e siti web o telefonici e anche mediante la rete di sportelli che forniscono informazioni sull'attività di FWA con logiche strettamente correlate alle finalità perseguite nei vari casi e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.
La conservazione dei dati personali di titolarità di FWA varia a seconda della tipologia e natura, oltre che dalle finalità perseguite nei vari trattamenti effettuati.
In ogni caso, in specifiche informative (cartacee o telematiche) ai sensi dell'art. 13 D.lgs. 196/2003 vengono fornite agli interessati (a seconda del trattamento) tutte le informazioni circa le finalità e le modalità perseguite nei singoli casi e in relazione agli specifici servizi forniti da FWA

La tabella contenuta nell'Allegato 2 "Catalogo Trattamenti", contiene la descrizione dei trattamenti - effettuati in formato cartaceo e con l'ausilio di strumenti elettronici anche ulteriori rispetto a quelli sopra indicati - specificando la natura dei dati trattati, la struttura organizzativa (interna o esterna) che effettua il trattamento, la descrizione e l'ubicazione degli strumenti utilizzati.

4. GESTIONE DEGLI INCARICATI

Sono di seguito descritti sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati FWA.

4.1. Distribuzione dei compiti e delle responsabilità

Il "**Titolare del trattamento**" dei dati: FWA di Milano, in persona del suo legale rappresentante pro tempore.

Il "**Referente per la protezione dei dati personali**" o "Referente Privacy" Dott. Romano Guerinoni.

Il trattamento dei dati personali viene effettuato dai Responsabili delle aree sopra individuate e da Dipendenti a ciò espressamente incaricati. FWA ha nominato specifici soggetti quali "Responsabili del trattamento dei dati" nella propria struttura (responsabili degli uffici Incaricati al trattamento dei dati) ai sensi dell'art. 29 D.lgs. 196/2003, in considerazione della loro esperienza, capacità ed affidabilità, tali da offrire idonea garanzia dei pieno rispetto delle disposizioni in materia di trattamento.
FWA intende mantenere aggiornato l'impianto delle responsabilità in ambito privacy e, pertanto, provvede a rendere disponibile un apposito elenco e documenti privacy presso la Direzione della Fondazione, intesi a identificare le figure incaricate, ad ogni ordine e grado, al trattamento e a fornire le istruzioni con specifiche policy interne.

FWA ha nominato per iscritto i Responsabili e gli Incaricati al trattamento secondo la natura e pertinenza dei dati rispettivamente trattati, nonché ha provveduto (laddove è risultato necessario) al rispettivo rinnovo e aggiornamento periodico annuale dell'individuazione dell'ambito del trattamento consentito. Tali istruzioni sono fornite, oltre che con lettera di incarico, anche attraverso la presa visione e accettazione di policy interne sulla sicurezza.

4.2. Responsabilità di processo e di gestione

FWA attua una rigorosa policy di classificazione e gestione del patrimonio informativo aziendale che attribuisce ad ogni ruolo aziendale precisi compiti e responsabilità, anche in materia di trattamento dei dati.

Tutte le persone fisiche all'interno di.FWA sono state autorizzate a compiere operazioni di trattamento direttamente dal Referente Privacy e/o dal proprio Responsabile del trattamento di area. Cadenziato l' aggiornamento nell'ambito del trattamento dei dati nei confronti degli Incaricati e la verifica delle condizioni dei profili di autorizzazione e di qualsiasi cambiamento che comporti la modifica dell'ambito di trattamento o la tipologia dei dati trattati all'interno delle singole unità o uffici verrà tempestivamente comunicato agli Incaricati per mezzo di circolari, comunicazioni, e-mail etc..

Tutti gli Incaricati sono nominati tali per iscritto ed ricevono precise istruzioni in merito alla corretta gestione e trattamento dei dati personali (anche mediante policy interne).

A seguito dell'entrata in vigore del Provvedimento del Garante del 27 novembre 2008 relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", è, altresì, comunicata una nuova informativa ex art. 13 a tutto il personale ed un elenco "Elenco degli amministratori di sistema". Tale documento, conservato presso FWA contiene, il nominativo delle persone fisiche operanti all' interno o all'esterno di FWA le quali, in qualità di Amministratori di Sistema, possono accedere ai dati personali di titolarità di FWA.

FWA ha provveduto alla designazione di un Referente Privacy (nella persona di Romani Guerinoni), ai sensi dell'art. 29 del D. Lgs. 196/2003 in relazione alle specifiche attività delegate e in considerazione della esperienza, capacità ed affidabilità espresse, tale da offrire idonea garanzia del pieno rispetto delle disposizioni in materia di privacy.

Ogni Responsabile ed Incaricato di FWA deve conoscere ed uniformarsi, conformemente alla formazione ricevuta, al rispetto sia di tutte le Policy aziendali sia di ogni precauzione ed attività nelle stesse contenute e, comunque, finalizzate alla corretta gestione dati personali trattati.

4.3. Procedura di gestione del Sistema di autenticazione e di autorizzazione

Tutti gli Incaricati, previa sottoscrizione di una informativa, sono nominati e autorizzati al trattamento dei dati (singolarmente o per classi omogenee) mediante lettera contenente specifici compiti e istruzioni; gli stessi sono autorizzati al trattamento dei dati per le sole finalità indicate da FWA (per il tramite del Responsabile di area/ufficio) ed è vietato qualsiasi altro uso dei dati personali trattati che non sia in linea con l'incarico ricevuto.

Gli Incaricati sono stati formalmente edotti in merito alla circostanza che:

a) il trattamento e la conservazione dei dati deve avvenire in modo lecito e proporzionato alle funzioni aziendali, nel rispetto della riservatezza;

b) la raccolta, registrazione ed elaborazione dei dati, mediante strumento elettronico o cartaceo, deve essere limitata alle necessità aziendali;

c) è onere dell'Incaricato la correzione od aggiornamento dei dati posseduti, l'esame della pertinenza rispetto alle funzioni;

d) è onere dell'Incaricato il rispetto dei compiti specifici che gli sono stati assegnati, nonché il rispetto delle istruzioni e delle modalità operative contenute nell'atto di conferimento dell'incarico (compreso le specifiche policy e linee guida richiamate).

Al momento della formalizzazione della nomina ad Incaricato, lo stesso riceve informazioni relativamente a:

- codice identificativo e password;
- uso delle password;
- back up dei dati aziendali rilevanti;
- policy di sicurezza a cui adeguarsi.

Il codice identificativo e la password non possono essere mai associati ad altri Incaricati e vengono disattivati se inutilizzati per 6 mesi o in caso di perdita della qualità di Incaricato.

A tutti gli Incaricati destinati al trattamento di dati mediante strumento elettronico sono state conferite credenziali di autenticazione (art. 34, comma 1, lett. b), mediante ID e parola chiave, conformi alla normativa e con l'obbligo di modificarle al momento della consegna ed aggiornarle periodicamente. Ogni Incaricato è custode e responsabile delle proprie password.

Ogni Dipendente, nominato Incaricato da FWA, risponde singolarmente, anche ai sensi del D.Lgs. 196/2003, di eventuali usi impropri dei dati e delle informazioni in particolare se, dal fatto, ne deriva un danno ovvero un vantaggio personale.

Il Responsabile del trattamento di area nominato deve adottare tutte le idonee azioni volte al mantenimento dell'informazione evitandone la diffusione indebita; come ogni Dipendente, il Responsabile risponde singolarmente, anche ai sensi del D. Lgs. 196/2003, di eventuali usi impropri dei dati e delle informazioni in particolare se, dal fatto, ne deriva un danno ovvero un vantaggio personale.

Al Referente Privacy, che coordina e supervisiona le Risorse Umane e l'organizzazione della Fondazione, di concerto con le funzioni apicali di FWA. e degli outsourcer delle soluzioni IT (es. DigiCamere e MGA Computer Service SRI), compete l'aggiornamento e la revisione del presente Manuale (e di tutte le policy collegate in materia sicurezza), la gestione e la responsabilità "in primis" di tutto il processo organizzativo, di controllo, di monitoraggio e di adeguamento strutturale, in materia di protezione dei dati personali.

4.4. Amministratori di sistema

FWA ha individuato in DigiCamere e MGA Computer Service srl, mediante specifiche lettere di nomina che rispettano i criteri di cui all'art. 29 d.lgs. 196/2003, i soggetti deputati a svolgere il servizio di "amministrazione di sistema", scegliendo tali soggetti per le garanzie di esperienza, capacità e affidabilità possedute; l'elenco degli amministratori di sistema (persone fisiche) e l'area aziendale di appartenenza è riportato all'interno di un documento "Elenco degli amministratori di sistema". Tale documento è conservato

presso le rispettive sedi delle società indicate ed è reso disponibile su semplice richiesta in caso di eventuali accertamenti o su richiesta dei partner istituzionale/commerciali di FWA.
L'operato degli amministratori di sistema e il controllo circa la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti è demandato a specifiche funzioni esterne dei soggetti nominati.
Viene verificato che le attività svolte dagli amministratori di sistema siano conformi alle mansioni attribuite mediante lettera di nomina, ivi compreso il profilo relativo alla sicurezza.

A tal fine, i soggetti esterni sopra menzionati sono dotati di un sistema che consente la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione (client, server, apparati di sicurezza, apparati di rete etc.) e agli archivi elettronici (file, database, posta elettronica, gestionali, ERP, log etc.) effettuati da parte degli amministratori di sistema (persone fisiche).

Alle registrazioni (access log) vengono garantite caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste, ovvero per verificare eventuali abusi e/o violazioni della riservatezza dei dati da parte di Amministratori di Sistema.

5. MISURE DI SICUREZZA

In questa sezione sono riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

In relazione al trattamento dei dati personali è, quindi, costantemente in atto un procedimento di controllo e di verifica della sicurezza del sistema informatico attraverso l'utilizzo di appositi strumenti a livello di sistema, di gestione delle basi dati e di applicativo (per ulteriori specifiche far riferimento al documento dell'analisi dei rischi), effettuato anche mediante l'ausilio di soggetti terzi (es. DigiCamere, MGA Computer Service srl).

5.1. Individuazione degli attacchi

L'individuazione degli attacchi deriva da una fase di analisi della realtà aziendale, che consta nella rilevazione dello scenario di riferimento, sia per quanto riguarda l'architettura informatica, sia per l'individuazione degli eventuali trattamenti che prevedono l'impiego di archivi di tipo cartaceo. In base a quanto rilevato, le componenti soggette a rischio risultano essere:

- ✓ reti e apparati di rete;
- ✓ elaboratori e software di sistema;
- ✓ software applicativo;
- ✓ supporti informatici di memorizzazione;
- ✓ infrastrutture;
- ✓ archivi cartacei;
- ✓ archivi di Backup.

Per contenere i rischi aventi impatto negativo sulla sicurezza dei dati, ogni funzione applica quanto contenuto nelle varie Policy aziendali, nonché in ogni altra linea guida utilizzata in favore dell'azienda.

5.2. Policy di Back up

Per tramite dei suoi outsourcer (DigiCamere e MGA Computer Service srl), FWA adotta procedure per il salvataggio dei dati al fine di garantirne il corretto e tempestivo ripristino in caso di danneggiamento o perdita di integrità dei dati.
Le policy di back up sono descritte in una policy specifica denominata "procedure di backup" elaborata e conservata presso la sede di Fwa .
I sistemi sono generalmente ospitati su server ad alta disponibilità che offrono una buona resilienza a situazioni di normali guasti tecnici e con dischi ridondati permettono di ripristinare la disponibilità dei dati in

caso di guasto.

A tal fine vengono effettuate le seguenti operazioni:
a) esecuzione giornaliera del back up attraverso procedure automatiche (notturno);
b) report dei back up effettuati;
c) archiviazione e verifica della procedura di ripristino dai supporti di back up.

Il back up della posta elettronica, invece, avviene sui server di Google (vd. contratto di "Fornitura di caselle di Posta Elettronica e servizi aggiuntivi Google" sottoscritto con Digicamere). Con riferimento a tale procedura si rinvia ai termini di servizio di Google (https://support.google.com/a/answer/60762?hl=it), che si ritiene rappresentino una sufficiente e adeguata garanzia di salvataggio dei dati ai sensi dell'art. 34, comma 1, lett. f) del d.lgs. 196/2003.

5.3. Misure di protezione

Sulla base degli attacchi individuati e delle necessità di protezione espresse dai requisiti precedentemente descritti, sono state adottate un insieme di misure di protezione così classificabili:

- ✓ **Misure di tipo organizzativo**. Rientrano in tale categoria:
  - le misure per l'assegnazione di compiti e responsabilità (nomine);
  - le misure per l'aumento della sensibilità aziendale nei confronti delle tematiche di tutela dei dati (formazione);
  - le misure per evitare l'attuazione di trattamenti di dati personali per finalità diverse da quelle autorizzate e consentite;
  - le misure per la protezione di archivi cartacei

- ✓ **Misure di protezione delle aree e dei locali (criteri di protezione fisica)** e rispettive procedure. Rientrano in tale categoria:
  - le misure per la protezione dall'accesso intenzionale e non autorizzato ai locali e agli archivi (anti-intrusione);
  - le misure per la protezione dei locali dall'accesso non autorizzato (intenzionale o non intenzionale) tramite le vie di accesso predisposte (controllo accesso);
  - le misure per la protezione dei dati da eventi di origine naturale o dolosa (antincendio);
  - le misure per la protezione da condizioni ambientali proibitive o da eventuali riduzioni dell'efficienza dei sistemi di supporto (impianti ausiliari).

- ✓ **Misure di protezione delle architetture di rete, degli applicativi e delle banche dati** (criteri di protezione logica dei dati) e relative procedure. Rientrano in tale categoria:
  - le misure per la protezione da accessi non autorizzati ad informazioni riservate (User-id, password, screensaver con password);
  - le misure per la protezione da possibili danneggiamenti alle informazioni (antivirus);
  - le misure per la protezione da eventuali perdite di disponibilità dei dati (back up completo giornaliero dei file server, mail server, application server ect.);
  - le misure necessarie finalizzate alla registrazione degli access log degli amministratori di sistema in ottemperanza al provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".

- ✓ **Misure di protezione durante la trasmissione dei dati** e relative procedure.

- ✓ Rientrano in tale categoria:
  - le misure per la trasmissione sicura delle informazioni su rete;
  - le misure per il trasferimento di dati mediante mezzi differenti dagli elaboratori.

La bontà delle misure adottate è periodicamente verificata secondo la seguente tabella:

Attività	Verifiche	Periodicità	Riferimento

			normativo
Individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici	A cadenza almeno annuale viene verificato l'aggiornamento periodico delle lettere di incarico e dei profili di autorizzazione	Annua	Allegato B al D. Lgs. n.196/03
Misure contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale		Giornaliera	Allegato B al D. Lgs. n.196/03
Misure volte a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti		Giornaliera	Allegato B al D. Lgs. n.196/03
Salvataggio dei dati	Frequenza giornaliera con procedure automatiche	Giornaliera	Allegato B al D. Lgs. n.196/03
Misure e accorgimenti, prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema	Controllo delle registrazioni degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici effettuati da parte degli Amministratori di Sistema e Audit Interno sullo stato di applicazione delle misure organizzative e tecniche di sicurezza	Annua	Provvedimento del Garante Privacy del 27 novembre 2008 e successive modifiche

Piano di verifica periodico delle misure adottate

Di seguito vengono descritte le misure di sicurezza atte a garantire:

- la protezione delle aree e dei locali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza nell'ambito dell'utilizzo degli strumenti elettronici.

Per quanto concerne il rischio d'area legato ad eventi di carattere distruttivo, gli edifici e locali nei quali si svolge il trattamento dei dati sono protetti da:

- dispositivi antincendio;
- impianto di condizionamento;
- impianto elettrico dotato di misure salvavita atte anche ed evitare cortocircuiti e possibili incendi.

Climatizzazione dei locali: i locali sono climatizzati. Per l'esatta indicazione delle misure di protezione (organizzative e di sicurezza) adottate, si rinvia alla specifiche policy e procedure interne adottate da DigiCamere e MGA SRL (responsabili esterni del trattamento), e allegate al presente Manuale (Allegato 4). Tale documento, infatti, rappresenta una sintesi delle misure di sicurezza delle quali DigiCamere ed MGA garantiscono l'applicazione anche per la specifica realtà della di FWA
Per l'applicazione e descrizione delle ulteriori misure di sicurezza hardware e software si rinvia altresì all' Allegato 3 "Capitolato tecnico d'appalto" del fornitore esterno MGA Computer Service srl, responsabile della sicurezza informatica e garante della conformità alle norme e standard di sicurezza in ambito IT (es. ISO/IEC 27001:2005, d.lgs. 196/2003, etc.). MGA Computer Service srl , in particolare, mantiene un inventario aggiornato degli hardware e software forniti e installati presso FWA.

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si effettua il trattamento dei dati sono protetti da:

- sistemi di allarme e di sorveglianza anti-intrusione (con registrazione dei codici di ingresso e registrazione degli eventi nel tempo);
- porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee;
- limitazioni all'accesso del data center (localizzazione del server);
- accesso controllato, mediante servizio di guardiania e portineria ;
- vigilanza che interagisce con il personale di FWA o videosorveglianza;
- in ciascun ufficio sono presenti armadi, schedari e cassetti dotati di chiusura a chiave, nei quali sono custoditi documenti cartacei contenenti dati personali;
- procedura di identificazione dei visitatori.

Dispositivi antincendio (estintori, manichette, impianti di rilevazione e/o spegnimento automatico):

1. antincendio a Gas nei locali interni;
2. estintori distribuiti in tutto l'edificio.
3.

5.4. Procedure interne volte alla gestione dei codici di identificazione

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 1, 2, 3, 6,7,8)*

Il trattamento dei dati personali, con strumenti elettronici, è consentito esclusivamente agli Incaricati dotati di credenziali di autenticazione. Le credenziali di autenticazione sono individuali ed identificano univocamente l'Incaricato sui sistemi di elaborazione cui ha accesso.
Ad ogni Incaricato è associato un profilo che gli consente l'accesso ad uno o più specifici trattamenti in base alle funzioni cui egli è preposto.
È compito degli Amministratori di Sistema approntare gli strumenti ed i controlli mediante cui verificare il corretto uso delle credenziali di autenticazione, nonché monitorare e vigilare sui tentativi di accesso non autorizzato.
In caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali, si procede alla verifica del profilo (cessazione attività o cambio di ruolo).
Le credenziali di autenticazione non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Esiste una procedura di disattivazione delle credenziali in caso di dimissioni di un Incaricato al trattamento dei dati personali.
FWA deve dare informazione a Digicamere e a MGA srl circa le dimissioni del personale o lo spostamento di mansione per annullare le credenziali di autenticazione dell'Incaricato del trattamento.
Nel caso in cui un Responsabile di area di FWA richieda una modifica rispetto alla configurazione dell'accesso al file server da parte di un Dipendente, tale richiesta va rivolta a Digicamere e MGA Computer Service per conoscenza va inviata al Referente (Romano Guerinoni).

5.5. Gestione, custodia e aggiornamento della parola chiave (Password)

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 4,5,9)*

Tutte le stazioni di lavoro sono protette da una username e password, così come per l'accesso ai server, che rispetta i requisiti minimi di complessità (8 caratteri alfanumerici con lettere maiuscole e minuscole) e che viene regolarmente cambiata ogni 90 giorni. Tutte le operazioni, riguardanti la gestione delle password svolte nel sistema informativo dagli utenti, vengono registrate in un file di registro (ogni pc ha memoria dell'evento "modifica psw" per un periodo di tempo ben definito oltre il quale vengono sovrascritte; si ha traccia anche delle stesse password su domain controller, ma in entrambi i casi citati le informazioni sono

crittografate e, pertanto, nessuno può accedere alle password utilizzate dall'utente).

La password di accesso presenta le seguenti caratteristiche:
a) Non corrisponde al nome utente o ai dati personali dell'utente;
b) Ha una lunghezza di almeno otto caratteri alfa-numerici;
c) Non corrisponde ad una semplice parola rintracciabile in un dizionario;
d) Non contiene riferimenti agevolmente riconducibili all'Incaricato.

Definizione delle credenziali di autenticazione, individuate tra le seguenti tipologie:
- Codice identificativo, più parola chiave;
- Il sistema principale di gestione dell'autenticazione avviene tramite l'interfaccia utente del sistema operativo tramite procedura di log-in, la sicurezza del sistema è garantita da Digicamere, che gestisce in Dominio per conto di FWA.

Le regole per la gestione della parola chiave sono le seguenti:
- Scadenza dopo 3 mesi di utilizzo;
- Non è possibile reintrodurre la password precedente (memorizzazione delle 2 ultime chiavi);
- Almeno 8 caratteri;
- Presenza di numeri o caratteri speciali necessaria;
- Scadenza dell'account utente dopo 6 mesi di inutilizzo.

Modalità di attivazione, variazione e gestione delle password:
a) l'attivazione della parola chiave è fatta da chi si occupa dell'amministrazione del sistema e l'utente è obbligato a modificare tale parola chiave al primo utilizzo del suo account;
b) è sempre possibile la modifica in via autonoma della parola chiave da parte dell'utente;
c) è possibile forzare (resettare) la parola chiave da parte dell'amministratore di rete portando a conoscenza dell'utente la forzatura effettuata nel caso fosse necessario.

Il processo di autenticazione consente di ottenere agli Incaricati uno specifico insieme di privilegi di accesso ed utilizzo rispetto alle risorse del sistema informatico.

Gli Incaricati al trattamento dei dati, osservano le seguenti istruzioni per l'utilizzo degli strumenti informatici:
- obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password);
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo assoluto di riservatezza;
- divieto di divulgazione della password di accesso al sistema (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano essi colleghi, responsabili del trattamento, amministratori di sistema, etc.).

Ad ogni Incaricato è imposto l'aggiornamento periodico della password con sistema automatico.

5.6. Sistema di assegnazione e controllo dei profili

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 12,13,14)*

Ogni Incaricato ha un proprio profilo di autorizzazione e può accedere ai soli dati a lui consentiti o per semplicità di gestione amministrativa, può accedere ai soli dati consentiti alla classe omogenea di incarico alla quale appartiene (es. admin, operatore vobis, operatore banca, admin banca ecc..). Tali profili autorizzativi sono configurati sugli appositi strumenti di sicurezza e di controllo delle autorizzazioni, delle piattaforme elaborative elettroniche.

I profili di autorizzazione, per ciascun Incaricato o per classi omogenee di Incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Il processo di assegnazione del profilo di autorizzazione avviene con queste modalità:

- consegna dell'informativa e delle policy sull'uso appropriato delle credenziali utente;
- creazione del profilo di autorizzazione sui sistemi;
- consegna delle credenziali e password.

In conformità a quanto disposto dal punto 4 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.lgs. n.196 del 30 giugno 2003), gli Incaricati debbono adottare le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica.

5.7. Misure di prevenzione da programmi dannosi o da accessi abusivi

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 16,17,20)*

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante un Sistema Antivirus aggiornato giornalmente , previa disponibilità degli aggiornamenti. L'aggiornamento avviene in modalità automatica. Nel caso venga riscontrata la presenza di virus informatici, si attiva una specifica procedura di gestione delle minacce.
In particolare, l'antivirus si attiva automaticamente in presenza di virus. Nel caso in cui il problema non venga neutralizzato in prima battuta, poiché può accadere che la rilevazione provenga dall'utente che - a causa del virus – ha riscontrato un problema, viene aperto uno specifico ticket. Può accadere, altresì, che MGA Computer Service srl rilevi un allarme del sistema e intervenga direttamente sui sistemi di FWA Per l'applicazione e descrizione delle ulteriori misure di sicurezza hardware e software si rinvia altresì all'Allegato 3 "Capitolato tecnico d'appalto" del fornitore esterno MGA srl, responsabile della sicurezza informatica e garante della conformità alle norme e standard di sicurezza in ambito IT (es. ISO/IEC 27001:2005, d.lgs. 196/2003, etc.).

5.9. Misure a protezione dei dati sensibili degli Interessati

I dati personali comuni (ed eventualmente quelli sensibili) degli Interessati ospitati su strumenti elettronici di FWA sono protetti mediante l'adozione di tecniche di cifratura e/o di anonimizzazione, nonché attraverso la distruzione dei supporti rimovibili sui quali eventualmente tali dati sono stati salvati.

La procedura di distruzione dei supporti rimovibili (apparecchiature hardware) di proprietà di FWA avviene per il tramite della società MGA srl, nel rispetto del provvedimento dell'Autorità Garante "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008.

5.10. Archivi cartacei

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 27,28,29)* 20

All'interno di FWA vengono trattati e/o conservati i documenti che possono contenere dati personali degli Interessati. L'archivio cartaceo viene comunque gestito nel pieno rispetto delle idonee misure di sicurezza in relazione al tipo di documentazione in esso contenuta.

Gli eventuali atti e documenti contenenti dati personali sensibili e/o giudiziari sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti; i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
L'accesso agli archivi contenenti dati sensibili e/o giudiziari è controllato ed consentito solo agli incaricati a ciò espressamente autorizzati.

Quando gli archivi non sono dotati di strumenti per il controllo degli accessi, le persone che vi accedono sono preventivamente autorizzate.

La documentazione aziendale di carattere riservato o contenente dati sensibili viene conservata all'interno di armadi con serratura.
Gli archivi cartacei vengono gestiti secondo le seguenti modalità:
- possono accedere alle informazioni contenute nell'archivio cartaceo solo i Responsabili designati e gli Incaricati da questi autorizzati con lettera scritta;
- l'accesso alle informazioni è consentito limitatamente ai soli dati personali la cui conoscenza è strettamente necessaria per lo svolgimento dei compiti assegnati;
- tutti i documenti che contengono dati personali sono conservati in archivi ad accesso selezionato.

Modalità di identificazione e registrazione degli accessi ai dati particolari dopo l'orario di chiusura: non esiste un sistema di controllo degli accessi che permette di registrare tempi di ingresso dei vari Dipendenti oltre all'orario di ufficio in quanto, per policy aziendale, nessuno può accedere oltre gli orari di apertura dell'edificio. In ogni caso, vi è la presenza di guardie all'ingresso che presidiano gli accessi alla struttura.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici, pertanto, Responsabili e Incaricati del trattamento dei dati personali sono stati istruiti per l'osservanza delle ulteriori e seguenti disposizioni:

- i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali e, nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- i faldoni contenenti i dati sono archiviati in una forma che non consenta l'identificazione dell'interessato a chi non autorizzato e comunque per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e successivamente trattati.
- per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, il Responsabile o l'Incaricato del trattamento non dovrà lasciarli mai incustoditi;
- il Responsabile o l'Incaricato del trattamento deve, inoltre, controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri;
- al termine dell'orario di lavoro tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, devono essere riportati nei locali individuati per la loro conservazione;
- i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi nelle postazioni di lavoro durante l'orario di lavoro;
- si deve adottare ogni cautela affinché ogni persona non autorizzata non venga a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici;
- per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche;
- particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura;
- è tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del luogo di lavoro.

6. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

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

In ambito sicurezza delle informazioni e Privacy, in ragione delle lettere di incarico e di nomina conferite a tutti i soggetti che trattano dati personali infatti, saranno predisposte sessioni formative e la relativa documentazione in cartaceo sarà disponibile presso l'ufficio Direzione Generale - Anna Heidi Ceffa,

consentirà di accrescere le proprie competenze e di riflesso migliorare la gestione delle informazioni aziendali.
Il Referente Privacy, in collaborazione con i Responsabili degli specifici trattamenti di dati personali della varie aree aziendali, valuta per ogni incaricato (o classe omogenea di incaricati) a cui è stato affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione specifici.

La formazione dei Responsabili e Incaricati al trattamento dei dati è programmata già al momento dell'ingresso in servizio; tale formazione, oltre a fornire le competenze e gli strumenti operativi per svolgere le proprie mansioni quotidiane, fornisce le informazioni necessarie per gestire le informazioni in conformità con la legge sulla privacy e sensibilizza tali soggetti sulla corretta condotta da seguire per la salvaguardia della riservatezza dei dati.
Coerentemente con l'evoluzione degli strumenti tecnici adottati e/o dall'insorgere di nuove disposizioni legislative in materia, verranno istituiti nuovi incontri formativi.

7. CONTATTI

I seguenti contatti saranno di aiuto nei casi sotto indicati:

Problematiche di utilizzo dei software, hardware e dispositivi informatici in genere, problematiche legate alle password e in generale di accesso ai sistemi di FWA, problematiche legate al proprio account e alla posta elettronica, problematiche legate alla navigazione web e ai tool aziendali.

Responsabile Privacy – Segreteria Generale (Heidi Ceffa– heidi.ceffa@fwamilano.org – (Orario 9.00 – 18.00) Telefono - +39 02.87198053.

Tali contatti sono utilizzabili anche per consigli relativi al miglioramento della sicurezza delle informazioni.

8. REVISIONI E ALLEGATI

Il presente documento, contenente una descrizione di tutte le procedure e misure di sicurezza di cui agli art. 31 e ss. del D.lgs. 196/2003 e dell'Allegato B viene sottoposto a revisione annuale nella sua interezza o in presenza di modifiche sostanziali nell'organizzazione e nell'adozione delle misure di sicurezza fisica e logica.

REVISIONI

N°	ATTIVITÀ	FUNZIONE	DATA	NOME
1	REDATTO DA	Responsabile Privacy Area Segreteria Generale Anna Heidi Ceffa	20.07.2015	Manuale sulle Misure di Sicurezza e Organizzative in ambito privacy
2	REVISIONE			

ALLEGATI

N°	NOME	DATA	AGGIORNATO AL
1	Organigramma privacy FWA	20.07.2015	01/10/2017
2	Nomine a incaricati, responsabili e amministratori di sistema (interni ed esterni	20.07.2015	
3	Architettura client/server con policy di sicurezza informatiche adottate da FWA	20.07.2015	
4	Inventario sistemi FWA		
5	Elenco Utenti FWA- Struttura file server policy – Elenco sportelli		
6	Check list amministratori di sistema	20.07.2015	
7	Informativa dipendenti	20.07.2015	