Misure di sicurezza Privacy		
RP1	Backup/continuity	Il backup dei dati deve essere periodico (almeno settimanale).
RP2	Backup/continuity	Deve essere definito un insieme di regole e procedure per assicurare che venga eseguito un backup adeguato alle necessità dell'organizzazione aziendale. Una politica di backup definisce il tipo (es. full o incrementale) di backup, la frequenza (generalmente giornaliera), e include le regole per verificare la rispondenza del processo di restore.
RP3	Gestione Media	Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
RP4	Gestione Media	I supporti rimovibili contenenti dati personali, sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
RP5	Gestione Password	Deve essere utilizzato un sistema di User id e password per l'identificazione e l'autenticazione degli utenti e degli amministratori.
RP6	Gestione Password	Deve essere data la possibilità all'utente di cambiare autonamente la propria password o il PIN, nel rispetto delle politiche prestabilite per la definizione della password stessa.
RP7	Gestione Password	La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
RP8	Gestione Password	La sostituzione delle password degli utenti deve essere richiesta dal sistema almeno ogni 180 giorni per i dati personali ordinari e 90 per i dati sensibili o giuridici.
RP9	Gestione Password	L'utenza che non accede al sistema per un periodo superiore a 6 mesi deve essere disattivata (la sua abilitazione deve richiedere l'intervento di un amministratore). Per l'ambito privacy il periodo di inattività è sei mesi, per tutti gli atri contesti può essere lungo fino a un massimo di 18.
RP10	Gestione Password	Deve essere prevista una procedura per tutti gli utenti che indichi le modalità da seguire in merito all'uso della password.
RP11	Gestione Password	E' necessario adottare una procedura per garantire la disponibilità dei dati in caso di assenza prolungata dell'incaricato. (Es. copia delle credenziali in cassaforte o impostazione di una nuova password da parte di un utente amministratore; comunicazione all'incaricato)
RP12	Antivirus	Deve essere installato il software antivirus in tutti i sistemi che possono essere colpiti dai virus (in particolare, PC e server).
RP13	Gestione Password	L'utente deve essere obbligato a cambiare la password al primo accesso.
RP14	Gestione Password	Deve essere imposto un formato della password per evitare l'utilizzo di password banali o che contengano riferimenti agevolmente riconducibili all'utente.
RP15	Gestione Rete	Deve essere utilizzato un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna.
RP16	Antivirus	Assicurarsi che tutti i meccanismi antivirus, firewall ed altri programmi per la sicurezza siano aggiornati (almeno semestralmente) ed eseguiti correttamente e che generino audit log. Controllare costantemente gli aggiornamenti di sicurezza per tutti i prodotti.
RP17	Gestione Rete	Devono essere utilizzati strumenti IDS automatici di analisi delle azioni effettuate sulla rete, sui sistemi e sulle applicazioni che evidenzino gli eventi o sequenze di eventi (anche se effettuati da più individui) che presentano caratteristiche predefinite e rappresentanti possibili attacchi al sistema (signatures). e che le evidenzino on-line alle stazioni di lavoro specificate. Tali strumenti devono essere disponibili e documentati. Questi sistemi si basano su un'analisi di "signatures", oppure sulle discordanze rispetto all'attività usuale.
RP18	Gestione SW/HW	Assicurarsi di installare tutte le patch di protezione disponibili per i componenti del sistema e i programmi software in uso. Installare le patch di protezione tempestivamente.
RP19	Gestione SW/HW	Il software deve essere aggiornato periodicamente, secondo le specifiche del fornitore in materia di sicurezza. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
RP20	Gestione utenze	Deve esistere una procedura per la gestione del ciclo di vita delle utenze (creazione, disabilitaizone temporanea, disabilitazione definitiva, modifica del profilo di autorizzazione); Ad un icaricato possono essere associati più credenziali di aut. (più login); la singola credenziale deve essere associata e riconducibile ad un singolo utente (non è permessa quindi la condivisione della conoscenza di credenziali di autenticazione).
RP21	Gestione utenze	Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
RP22	Gestione utenze	Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
RP23	Gestione utenze	Deve essere condotta periodicamente una revisione dei diritti di accesso assegnati ai singoli utenti (almeno una volta all'anno). Si consiglia di rivedere i diritti di accesso degli Amministratori con una frequenza maggiore.
RP24	Gestione utenze	I profili di autorizzazione vanno definiti e concessi in modo tale da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento
RP25	Sicurezza organizzativa	Deve essere indicato il Responsabile delle Informazioni, che sarà quindi responsabile della gestione degli accessi alle informazioni. Questi potrà delegare ad altri il mantenimento delle autorizzazioni (Amministratore di Sistema). Nessun altro potrà svolgere queste attività.
RP26	Sicurezza organizzativa	L'accesso alle informazioni deve essere adeguato alla classificazione delle stesse e il livello di classificazione deve essere evidenziato con opportuni meccanismi. Si pensi alla distinzione tra le varie tipologie di dati personali.
RP27	Cifratura/crittografia	Nel caso di utilizzo per fasi di sviluppo e test di dati personali di natura particolare e giudiziaria, il set di dati devono essre deidentificati e desensibilizzati in modo che le informazioni sensibili risultino anonime.
RP28	Cifratura/crittografia	I dati personali di natura particolare e giudiziaria devono essere protetti mediante pseudonimizzazione (conservare i dati in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive).