MISURE DI SICUREZZA LIVELLO DI RICHIO BASSO (LOW)	
L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	
La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.	
I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	
In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.	
I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.	**compatibilmente con le modalità disponibili sulle piattaforme del cliente**
L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	**non facciamo**
Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	
L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	
Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	**non facciamo**
personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare	**non abbiamo contratti diretti**
Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	

Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	**che cosa dobbiamo fornire ?**
È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	
Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.	
L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).	
L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di preassunzione e / o assunzione.	
L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	
Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	**non facciamo e dipendono dalle modalità disponibili sulle piattaforme del cliente**
L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	
Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	
Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	**compatibilmente con le modalità disponibili sulle piattaforme del cliente**

Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	**compito delle piattaforme esterne**
I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento	**compito delle piattaforme esterne**
I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	**compito delle piattaforme esterne**
I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR) .	**compito delle piattaforme esterne**
Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	
Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base settimanale.	
Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	
Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	**compatibilmente con le modalità disponibili sulle piattaforme del cliente**
Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	**se compatibile con il funzionamento del sito**
Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	
Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	**dipendono da piattaforma esterna del cliente**
Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	**dipendono da piattaforma esterna del cliente**
L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	

I backup completi devono essere eseguiti regolarmente.	
Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	**compatibilmente con le modalità disponibili sulle piattaforme del cliente**
I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere preregistrati e preautorizzati.	**compatibilmente con le modalità disponibili sulle piattaforme del cliente**
I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.	**compatibilmente con le modalità disponibili sulle piattaforme del cliente**
Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.	**Cioè ?**
Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	
Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	
Dovrebbero essere seguiti standard e pratiche di codifica sicure.	**Cioè ?**
Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.	
La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.	**dipendono da piattaforma esterna del cliente**
È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	
Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	