Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Data Privacy Compliance (GDPR)

Redatto da:	**Accenture**
In Data	**Aprile 2022**

Aggiornamenti e Modifiche:

Versione finale	**22 Aprile 2022**

Indice

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Introduzione

Il presente documento descrive nel dettaglio i diversi aspetti per cui il servizio risulta conforme agli obblighi e agli adempimenti previsti dalla normativa GDPR e nazionale in materia di protezione dei dati personali. In particolare, saranno di seguito dettagliate le modalità di conservazione ed eventuale archiviazione dei dati, le misure di sicurezza predisposte in caso di accesso non autorizzato e gli strumenti a disposizione attraverso cui è possibile monitorare i livelli di sicurezza dei dati, in osservanza delle policies aziendali.

Saranno, inoltre, descritte le tempistiche e le modalità di gestione e comunicazione ai soggetti interessati di eventuali violazioni dei dati (*Breach*), le modalità predisposte affinché sia possibile restringere l'accesso agli stessi e, infine, le previsioni contrattuali in tema di liability e/o eventuali coperture assicurative ad hoc concordate con il Cliente in relazione al rischio privacy.

1. Modalità di conservazione ed eventuale archiviazione dati

Nel presente documento saranno descritte le modalità di conservazione ed eventuale archiviazione dei dati adottate. In particolare, in merito alle modalità di memorizzazione viene utilizzato un approccio misto basato su un Private Cloud, di proprietà di Accenture, e un Public Cloud (AWS Amazon), per l'archiviazione dei documenti.

Al termine della scadenza contrattuale, concluse le attività di trasferimento dati al Cliente attraverso la predisposizione di canali sicuri (Share Point, One Drive, SFTP), per quanto concerne l'archiviazione, la stessa spetterà al Cliente o al Fornitore in base alle previsioni contrattuali e/o di legge e verrà effettuata nel rispetto delle disposizioni normative in materia.

Inoltre, ai sensi delle policies aziendali, in particolare relative al *Data Management*, è garantita una gestione che assicuri l'identificazione, classificazione e protezione di tutte le forme di dati personali,

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

confidenziali, aziendali e altri dati protetti o regolamentati, sia con riferimento ai dati di Accenture che ai dati dei Clienti.

In aggiunta, in compliance con la policy relativa al *Corporate Records and Information Management*, la gestione dei Corporate Records e dunque dei documenti aziendali elettronici e cartacei identificati nelle pianificazioni di conservazione dei record mira al mantenimento dei Records aziendali nelle ipotesi in cui è richiesto per scopi normativi, legali e operativi, ad assicurare la continuità e l'efficienza delle operazioni aziendali e a ridurre la conservazione dei documenti non più necessari alle finalità aziendali.

1.1. Consegna e/o archiviazione dati attraverso canali sicuri di trasferimento conformi alle policy aziendali

Per l'attività di consegna, il cliente deve predisporre un canale di trasferimento sicuro (ad esempio: Share Point, One Drive, SFTP), in linea con le policy aziendali (nr. 0056 – System Security), con la precisazione che si intendono non compliant con le suddette supporti esterni per il trasferimento dei fascicoli (quali dischi magnetici, USB, CD-ROM, altro…).

Qualora il Cliente non fornisse un proprio canale di trasferimento in linea con la suddetta policy, il Fornitore metterà a disposizione un Tool denominato "*Accenture External File Share (AEFS)*".

Nello specifico, AEFS consiste in una soluzione sicura per condividere file con utenti al di fuori del dominio Accenture in grado di prevenire la perdita di dati (Data Loss Prevention) al fine di salvaguardare determinati dati aziendali e dei Clienti proprietari dalla divulgazione non autorizzata o involontaria.

Verranno concordati con il cliente i tempi per effettuare l'estrazione dei dati residenti in piattaforma e le modalità di consegna degli stessi in conformità alle suddette Policies aziendali.

Nello specifico, l'Appaltatore fornirà, alla chiusura del Contratto, il servizio di estrazione dati (fascicoli di gara), relativo alle procedure presenti sul sistema, secondo modalità e criteri condivisi, di seguito, a titolo esemplificativo, dettagliati.

In particolare, in base alla tecnologia utilizzata, all'esito dell'estrazione dati e creazione fascicoli, potrà variare la struttura delle Folder.

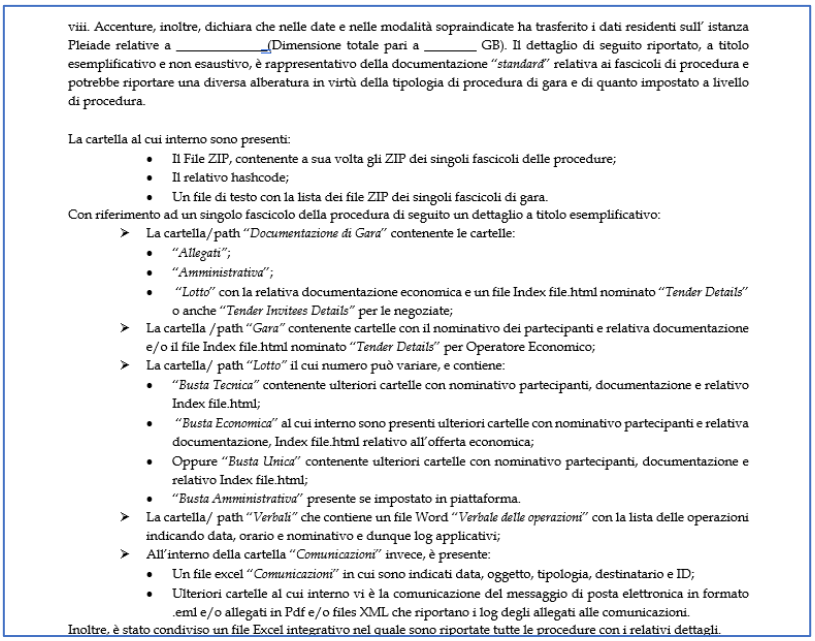
Di seguito sono elencati i formati in cui è possibile estrarre i dati:

- Csv;

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

- Rtf;
- Eml;
- Html;
- Pdf;
- Xls;
- Txt.

Di seguito e a titolo esemplificativo una print della struttura dati, di cui si dà evidenza nell'Appendice Tecnica condivisa con il cliente al momento della consegna:



viii. Accenture, inoltre, dichiara che nelle date e nelle modalità sopraindicate ha trasferito i dati residenti sull' istanza Pleiade relative a _____(Dimensione totale pari a _____ GB). Il dettaglio di seguito riportato, a titolo esemplificativo e non esaustivo, è rappresentativo della documentazione "*standard*" relativa ai fascicoli di procedura e potrebbe riportare una diversa alberatura in virtù della tipologia di procedura di gara e di quanto impostato a livello di procedura.

La cartella al cui interno sono presenti:

- Il File ZIP, contenente a sua volta gli ZIP dei singoli fascicoli delle procedure;
- Il relativo hashcode;
- Un file di testo con la lista dei file ZIP dei singoli fascicoli di gara.

Con riferimento ad un singolo fascicolo della procedura di seguito un dettaglio a titolo esemplificativo:

- La cartella/path "*Documentazione di Gara*" contenente le cartelle:
  - "*Allegati*";
  - "*Amministrativa*";
  - "*Lotto*" con la relativa documentazione economica e un file Index file.html nominato "*Tender Details*" o anche "*Tender Invitees Details*" per le negoziate;
- La cartella /path "*Gara*" contenente cartelle con il nominativo dei partecipanti e relativa documentazione e/o il file Index file.html nominato "*Tender Details*" per Operatore Economico;
- La cartella/ path "*Lotto*" il cui numero può variare, e contiene:
  - "*Busta Tecnica*" contenente ulteriori cartelle con nominativo partecipanti, documentazione e relativo Index file.html;
  - "*Busta Economica*" al cui interno sono presenti ulteriori cartelle con nominativo partecipanti e relativa documentazione, Index file.html relativo all'offerta economica;
  - Oppure "*Busta Unica*" contenente ulteriori cartelle con nominativo partecipanti, documentazione e relativo Index file.html;
  - "*Busta Amministrativa*" presente se impostato in piattaforma.
- La cartella/ path "*Verbali*" che contiene un file Word "*Verbale delle operazioni*" con la lista delle operazioni indicando data, orario e nominativo e dunque log applicativi;
- All'interno della cartella "*Comunicazioni*" invece, è presente:
  - Un file excel "*Comunicazioni*" in cui sono indicati data, oggetto, tipologia, destinatario e ID;
  - Ulteriori cartelle al cui interno vi è la comunicazione del messaggio di posta elettronica in formato .eml e/o allegati in Pdf e/o files XML che riportano i log degli allegati alle comunicazioni.

Inoltre, è stato condiviso un file Excel integrativo nel quale sono riportate tutte le procedure con i relativi dettagli.

Figura 1

Oggetto della consegna, dunque, saranno i dati estratti secondo le modalità indicate nel precedente paragrafo. Nel dettaglio, per ogni fascicolo di gara, verrà inviata la documentazione e le comunicazioni.

Nel modulo "*documentazione*" è presente la documentazione di gara, caricata dalla Stazione Appaltante, dall'Operatore Economico, i relativi lotti con Buste Tecniche/Economiche/Amministrative o busta unica e il verbale delle operazioni.

Il secondo modulo include le comunicazioni e la relativa documentazione allegata alle stesse suddivise in inviate e ricevute.

Si precisa, che la struttura sopra descritta, potrebbe subire variazioni in virtù della tecnologia utilizzata, della tipologia di procedura di gara e delle impostazioni a livello di procedura.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Nello specifico, i due moduli sopra indicati, consistono in due File zip (che presentano il Protocol ID/IDT e dunque un codice univoco che consente di identificare a che gara si fa riferimento).

Si segnala che la procedura relativa alla condivisione sicura della chiave/i di cifratura, necessaria alla consultazione/estrazione autonoma dei dati trasferiti al Cliente in formato Zip prevede che il

referente individuato dal Cliente riceva la chiave di cifratura trasmessa a lui esclusivamente nelle modalità concordate, in separato thread, per garantire la riservatezza delle informazioni.

Inoltre, è possibile implementare una funzionalità aggiuntiva in piattaforma, per la conservazione elettronica/digitale delle procedure di gara, presso un ente conservatore certificato, come da normativa AGID.
Si riportano a titolo di esempio per quanto concerne la conservazione elettronica digitale l'istanza SICP- Sistema Informatico Contratti Pubblici della Provincia Autonoma di Bolzano la piattaforma risulta integrata con l'ente conservatore ParER.

1.2. Accenture Data Management

La Policy aziendale 1431- Data Management, relativamente ai Dati di Accenture, stabilisce le responsabilità dei seguenti gruppi di dipendenti di Accenture, e descrive le azioni volte a garantire un'adeguata Protezione del Dato e quelle Correttive che gli stessi sono tenuti a intraprendere:

- Responsabilità dell' **Information Security Executive Sponsor e dell'Internal Information Security Lead**: gli stessi sono tenuti a comprendere la portata dei Dati Accenture per i quali sono responsabili, dimostrare l'osservanza dei propri obblighi relativi a tali Dati in conformità alle policies aziendali e, inoltre, a nominare un responsabile della sicurezza delle informazioni (SI).

  Quest'ultimo, all'interno del particolare mercato/unità di mercato, servizio, funzione aziendale o altra entità, dovrà provvedere ad istituire e mantenere un registro delle attività informative, nominare un Data Governor per ogni Asset informativo nell'Asset Register. Il Responsabile della Sicurezza delle Informazioni, inoltre, darà priorità agli Information Assets secondo la procedura di prioritizzazione definita e implementata dalla Information Security Corporate Function, considerando il valore dell'Information Asset per Accenture, il rischio che venga compromesso e, previa consultazione con i Legal Accenture, i rischi legali e relativi alla regolazione.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

- Responsabilità dei **Data Governors** in merito alle seguenti attività di protezione:
  - Classificazione degli Information Assets secondo gli Standard di Classificazione e Protezione Dati. La classificazione e la revisione deve essere svolta al momento dell'acquisizione o dello sviluppo, almeno una volta all'anno. Inoltre, eventuali modifiche al livello di classificazione potrebbero verificarsi in seguito a determinati eventi scatenanti (ad esempio: i bilanci classificati come dati riservati prima del deposito presso SEC diventano classificati come dati senza restrizioni una volta che sono archiviati presso SEC; oppure le richieste di modifica ai sistemi possono includere dati nuovi e sensibili che determinano una modifica della classificazione).
  - Gli Information Assets che contengono Dati Personali dovranno essere esplicitamente identificati nel Registro delle attività ed i relativi Data Governors dovranno ottemperare agli obblighi descritti nella Policy 0090 - Data Privacy, dettagliata nei prossimi paragrafi.
  - I Controlli Di Protezione che dovranno essere garantiti dal Data Governor sono relativi in primis all'Accesso e autenticazione. In particolare, gli Information Assets costituiti da documenti elettronici e supporti fisici devono essere etichettati con la loro classificazione in conformità agli Standard di Classificazione e Protezione Dati. I meccanismi di autenticazione descritti negli stessi devono essere utilizzati per controllare l'accesso alle risorse informative e gli elenchi di controllo degli accessi per le risorse di informazione devono essere definiti e implementati per i dati altamente riservati e i dati soggetti a restrizioni. Il controllo dell'accesso a tutte le informazioni sensibili deve essere periodicamente riesaminato in conformità ai già citati Standards e i singoli soggetti avranno accesso alla quantità minima di informazioni necessarie per svolgere le attività di propria competenza, rivedendo, inoltre, periodicamente l'autorizzazione all'accesso agli stessi (principio del "least privilege"). Gli utenti del sistema di ogni Asset Informativo devono, inoltre, disporre di account individuali, evitando la condivisione delle proprie password. In aggiunta, in merito alle attività di Stoccaggio e trasmissione gli Assets Informativi devono essere archiviati e/o trattati solo su un'infrastruttura approvata da Accenture. I Dati Accenture devono essere crittografati in conformità agli Standard di Crittografia e agli Standard di Classificazione e Protezione Dati quando sono conservati, trasmessi, trasportati o comunicati.
  - Con riferimento alle attività di Backup, conservazione e smaltimento, i dati nelle risorse informative devono essere sottoposti a backup in modo sicuro con una frequenza e una timeline di ripristino che supporti le esigenze aziendali. Si segnala, peraltro, che i Dati

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Aziendali contenuti negli Information Assets devono essere conservati in conformità alla Policy 0123 - Business Records and Information Management e alla Policy 1413 - Corporate Records and Information Management.

Al termine del proprio ciclo di vita, i dati elettronici o fisici contenuti negli Assets devono essere cancellati o smaltiti in modo sicuro o distrutti con appropriata autorizzazione, secondo gli Standard di Classificazione e Protezione Dati.

- Infine, in merito alle **Responsabilità del personale individuale**, gli stessi dovranno osservare, nello svolgimento delle attività di propria competenza, gli Standards di Classificazione e Protezione Dati sui materiali in loro possesso. Dovranno, inoltre, utilizzare le tecnologie disponibili (es. crittografia) per proteggere i dati e sarà vietato archiviare i Dati Accenture classificati come Riservati, Altamente Riservati o Riservati su dispositivi o supporti non crittografati, a meno dell'attivazione del processo per la concessione di eccezione. Sono inoltre predisposte attività di formazione in materia di privacy, protezione dei dati e sicurezza delle informazioni (Policy 0053 - Accesso del personale esterno ai sistemi Accenture, Policy 0056 - Sicurezza del sistema, Policy 0057 - Uso accettabile di informazioni, dispositivi e tecnologia, Policy 0069 - Riservatezza, Policy 0090 - Privacy dei dati e Policy 0123 - Business Records and Information Management). Il personale, in aggiunta, dovrà informare il Data Governor se ritiene di avere accesso a più informazioni di quelle necessarie per svolgere l'attività di propria competenza e dovrà contattare immediatamente il team Data Privacy per ricevere assistenza in caso di richieste di accesso ai Dati Accenture da parte delle forze dell'ordine. Infine, dovranno gestirei rischi di sicurezza delle informazioni relativi ai fornitori, in conformità alla Policy 0931 - Approvvigionamento di beni e servizi. Tutti i fornitori e i subappaltatori che archiviano, elaborano o trasmettono i Dati di Accenture e/o dei Clienti devono predisporre appropriate previsioni contrattuali in merito ai temi di Information Security negoziate come parte del contratto.

1.3. Data Privacy

L'obiettivo della Policy 0090I Data Privacy è:

- descrivere gli obblighi e gli impegni di Accenture per conformarsi all'etica e alle legislazioni sulla privacy dei dati;
- definire le responsabilità di ognuno in materia di privacy dei dati;
- regolare il modo in cui vengono gestiti i dati personali;
- identificare ulteriori risorse per aiutare i dipendenti a conformarsi a questa policy.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Accenture esprime il proprio impegno nella protezione dei dati personali e della privacy della persona nel nostro Codice di Etica Aziendale (COBE), nelle nostre norme vincolanti d'impresa e nei nostri accordi contrattuali con rivenditori, fornitori, partner e clienti. Accenture dispone di un programma globale per la privacy dei dati per gestire tale impegno e risolvere questioni legate a conformità, rischi e opportunità etiche e legali.

Inoltre, le leggi sulla privacy dei dati (in particolare il Regolamento generale per la protezione dei dati dell'Unione Europea (GDPR) regolano il modo in cui vengono gestiti i dati personali e definiscono i conseguenti obblighi legali.

L'applicabilità e portata della policy in esame concerne le ipotesi in cui Accenture è il titolare del trattamento e utilizza dati personali per i propri scopi (ad esempio per attività di reclutamento del personale, assunzione, marketing, intrattenimento aziendale, gestione di eventi, gestione di fornitori e rivenditori), mentre non trova applicazione nei casi in cui Accenture è Responsabile del trattamento per servizi forniti ai clienti e dunque relativamente ai dati personali di proprietà dei clienti su cui Accenture effettua trattamenti a nome dei clienti come parte dei servizi ad essi forniti.

Nei casi in cui Accenture agisce come responsabile del trattamento di dati personali di proprietà dei clienti, come si vedrà più nel dettaglio di seguito, Accenture dispone di un Programma per la protezione dei dati del cliente (CDP) con policy e procedure separate per implementare i requisiti della privacy dei dati applicabili ai dati di proprietà dei clienti. È infatti ingaggiato un team CDP dedicato, responsabile di fornire relative indicazioni e controlli in merito.

In merito alla gestione della privacy dei dati, Accenture si avvale di un team globale per la privacy dei dati, di un responsabile della protezione dei dati di Accenture, di responsabili della protezione e della sicurezza dei dati, di conformità geografica e responsabile legale aziendale, di asset stewards e di persone designate all'interno delle funzioni aziendali, ognuna con responsabilità e doveri specifici per la gestione della privacy dei dati.

Il trattamento dei dati personali dovrà essere effettuato in modo coerente con il Codice di Etica Aziendale (COBE), definendo gli obiettivi e limitando l'utilizzo dei dati personali agli stessi.

È possibile effettuare trattamenti di dati personali esclusivamente per scopi specifici, come definito dalla normativa vigente in ambito Privacy, a seguito di esplicito consenso esplicito da parte del titolare e con la chiara definizione delle finalità per cui i dati degli interessati vengono utilizzati.

In caso di ottenimento di dati personali da fonti esterne sarà necessario accertare con il Dipartimento Privacy la sussistenza di effettive basi legali per il trattamento degli stessi prima di utilizzarli.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Le notifiche fornite all'interessato devono essere in forma scritta, in accordo con le indicazioni di Accenture, utilizzando un linguaggio semplice per informare gli interessati dei motivi per cui i dati personali sono raccolti ed utilizzati, per quanto tempo e qualsiasi altra informazione rilevante.

Dovranno essere raccolti esclusivamente i dati personali rilevanti e limitarsi a quanto ragionevolmente necessario per raggiungere lo scopo prefissato. E', inoltre, necessario considerare la possibilità di utilizzare dati anonimi, pseudonimizzati o aggregati anziché dati personali e Accertarsi che i dati personali siano accurati, aggiornati e rilevanti per il raggiungimento dello scopo prefissato.

Ai sensi della policy non potranno essere conservati dati personali a tempo indeterminato o più a lungo del necessario e, in merito ai requisiti di conservazione e gestione degli archivi di Accenture il riferimento è la Policy 1413 e la Policy 1431 descritte all'interno del presente documento.

Inoltre, in compliance con le policies aziendali e con la normativa in materia, Accenture considera la privacy come parte integrante di progettazione, sviluppo, funzionamento e gestione di nuovi progetti, strumenti, applicazioni, servizi interni e offerte che utilizzano dati personali. Quando vengono coinvolti rivenditori o partner in qualsiasi parte del processo di progettazione, sviluppo e implementazione, anche la privacy già a partire dalla fase di progettazione risulta parte integrante del progetto.

Inoltre, alcuni tipi di attività di trattamento dei dati (ad esempio nuovi strumenti, app o servizi) richiedono di effettuare con anticipo una valutazione dell'impatto sulla protezione dei dati (Data Protection Impact Assessment - DPIA) o una revisione per contribuire a mitigare i rischi relativi all'ambito privacy. In base agli esiti della valutazione o della revisione, è necessario intraprendere azioni nel corso della progettazione o dell'implementazione dello strumento, applicazione o servizio offerto. Ciò può richiedere di mettere in atto ulteriori misure per la mitigazione dei rischi o restrizioni su alcuni aspetti del trattamento.

Accenture, inoltre, implementa misure per il controllo dell'accesso e per la protezione dei dati personali attenendosi ai protocolli di sicurezza di Accenture e a tutte le policy, procedure e indicazioni rilevanti per la sicurezza, inclusa la Policy 57 in tema di Uso consentito di informazioni, dispositivi e tecnologia.

Nell'ambito di attività di collaborazione con fornitori o rivenditori (responsabili del trattamento), sarà necessaria la predisposizione di accordi contrattuali specifici prima della divulgazione dei dati personali, nonché l'osservanza di tutti i protocolli di accesso e le restrizioni in merito alla divulgazione (applicabili per legge, contratto o per le procedure interne ad Accenture), anche in caso di condivisione dei dati con rivenditori e partner.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

1.4. Client Data Management

In conformità alla Policy sopra citata (Policy 1431- Data Management), con riferimento ai Dati del Cliente, viene predisposto il programma Client Data Protection (CDP) che definisce i requisiti specifici per i seguenti gruppi di dipendenti Accenture:

- Personale individuale
- Sales/Opportunity teams
- Client Delivery teams
- Strategic Business Initiatives, Acquisitions, Joint Ventures and Offerings teams

In particolare, il programma CDP stabilisce una metodologia e uno standard di condotta per il personale che accede, elabora, detiene, trasferisce o tratta in altro modo i Dati dei Clienti. Il programma CDP è progettato per aiutare i dipendenti a gestire i Dati dei clienti in conformità con i contratti dei clienti, le politiche di Accenture e la normativa europea e nazionale applicabile.

L'utilizzo dello strumento di valutazione del rischio CDP ha lo scopo di individuare:

- la natura e la portata dei Dati del Cliente a cui il personale avrà accesso;
- il livello di rischio regolamentare, finanziario, contrattuale e reputazionale che potrebbe essere associato alla perdita o all'uso improprio dei Dati del Cliente;
- il rischio operativo basato sulla portata dei servizi e sul modello di erogazione;
- I termini contrattuali necessari per la gestione di tali rischi e i soggetti che hanno approvato le attività richieste per le eventuali eccezioni alle condizioni contrattuali.

In base al punteggio di rischio calcolato automaticamente, si determineranno i processi specifici del programma CDP e i termini contrattuali richiesti.

Sulla base della valutazione del rischio, saranno conseguentemente predisposti opportuni controlli CDP, lavorando con il cliente per progettare una soluzione che riduca ragionevolmente il rischio di una divulgazione non autorizzata dei dati dei clienti.

Nel dettaglio, la soluzione deve contenere almeno i seguenti elementi:

- Accenture dovrebbe avere accesso solo alla quantità minima di Dati commerciali altamente riservati dei clienti e Dati personali dei clienti altamente riservati necessari per adempiere alle proprie responsabilità contrattuali.
- I dati di produzione non dovrebbero essere utilizzati in ambienti non di produzione. Se il cliente ordina ad Accenture di utilizzare i dati di produzione in ambienti non produttivi, il

team Sales/Opportunity deve includere nella soluzione opportuni controlli di compensazione e ottenere l'approvazione del rischio da parte del cliente.

- I dispositivi portatili, i laptop e i supporti che possono essere utilizzati per archiviare dati altamente riservati devono essere crittografati. Se i dispositivi o i supporti sono forniti dal cliente e non sono crittografati, è necessaria la conferma scritta dell'accettazione del rischio da parte del cliente.

Di seguito una Tabella riepilogativa relativa ai ruoli chiave e alle relative responsabilità in merito alla protezione dei Dati dei Clienti:

Sales/Opportunity Team	L'Accenture Leader del team deve garantire che il team identifichi i Dati del Cliente, utilizzi lo Strumento di Valutazione del Rischio CDP, includa i controlli CDP nella soluzione e includa i controlli CDP nel piano di mobilitazione dell'engagement.
Client Delivery Team	Il Leader Accenture del team deve garantire che il team crei, mantenga ed esegua i controlli CDP, in linea con il Piano CDP.
Accountable Managing Director (AMD)	Leader Accenture nel Client Delivery Team che comprende la natura e la portata dei servizi forniti al cliente, ha un rapporto di lavoro con il cliente e ha l'autorità e la responsabilità di garantire lo sviluppo, manutenzione e implementazione del programma CDP, del Piano CDP e dei controlli CDP.
Account Information Security Lead (A-ISL)	Viene affidata l'implementazione e gestione della compliance delle attività in corso con il programma CDP, sotto la direzione del Accountable Managing Director.

In merito all'accesso e utilizzo dei dati, in conformità al CDP Plan, sarà consentito l'accesso esclusivamente ai Dati del Cliente necessari per lo svolgimento delle attività di propria competenza. In particolari i dati del Cliente potranno essere utilizzati solamente al fine di fornire servizi contrattuali, come concordato nel contratto con il cliente o come indicato dal Team Legal di Accenture.

Inoltre, con riferimento alle attività di Conservazione e smaltimento, in conformità alle policy aziendali è garantito che le tempistiche di conservazione dei Dati dei clienti sui dispositivi non vadano oltre quanto necessario per svolgere le attività. Pertanto, si procederà ad eliminare,

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

distruggere o restituire attraverso canali sicuri al cliente tutti i Dati (elettronici e fisici) di sua proprietà, al termine della fornitura dei servizi, in conformità alle previsioni contrattuali e legali. Si provvederà, inoltre, ad eliminare tutti i Dati del Cliente da qualsiasi materiale condiviso o riutilizzato (inclusi i metadati per i documenti elettronici).

Si segnala che nelle ipotesi di Violazione della Sicurezza (Security Breach) si procederà immediatamente a segnalare i casi in cui vi è stato o potrebbe esserci stato un accesso inappropriato o una divulgazione non autorizzata dei Dati del Cliente. Le segnalazioni devono essere fatte all'Accenture Security Operations Center (ASOC), come descritto più nel dettaglio nei prossimi paragrafi, chiamando all'apposito recapito o attraverso una segnalazione online.

1.5. Accenture Client Data Protection

Il team di Information Security ha sviluppato e migliora continuamente il già citato programma globale Client Data Protection (CDP) che garantisce che i team comprendano e rispettino gli obblighi di privacy e sicurezza dei dati relativi a ciascun cliente. Come si accennava, il programma fornisce ai team strumenti e processi che consentono loro di identificare e mitigare i rischi per la sicurezza durante il ciclo di vita di un progetto e un approccio standardizzato per proteggere i dati dei clienti che include:

- un modello di responsabilità per la sicurezza delle informazioni all'interno di ogni progetto del cliente;
- controlli che proteggono i dati dei clienti quando sono visionati, gestiti, trasmessi, ospitati o archiviati, nonché controlli specifici legati ai rischi inerenti alla tipologia di attività svolte;
- tecnologie per proteggere i dati del cliente come: cifratura del disco rigido, scansione delle configurazioni relative alla postazione di lavoro e protezione dalla perdita di dati;
- training specifico dei team per rispondere ad esigenze del cliente ed a rischi specifici del progetto;
- subject matter expert che condividono le "best practices" e verificano l'efficacia delle pratiche e dei controlli di sicurezza adottati dal team.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

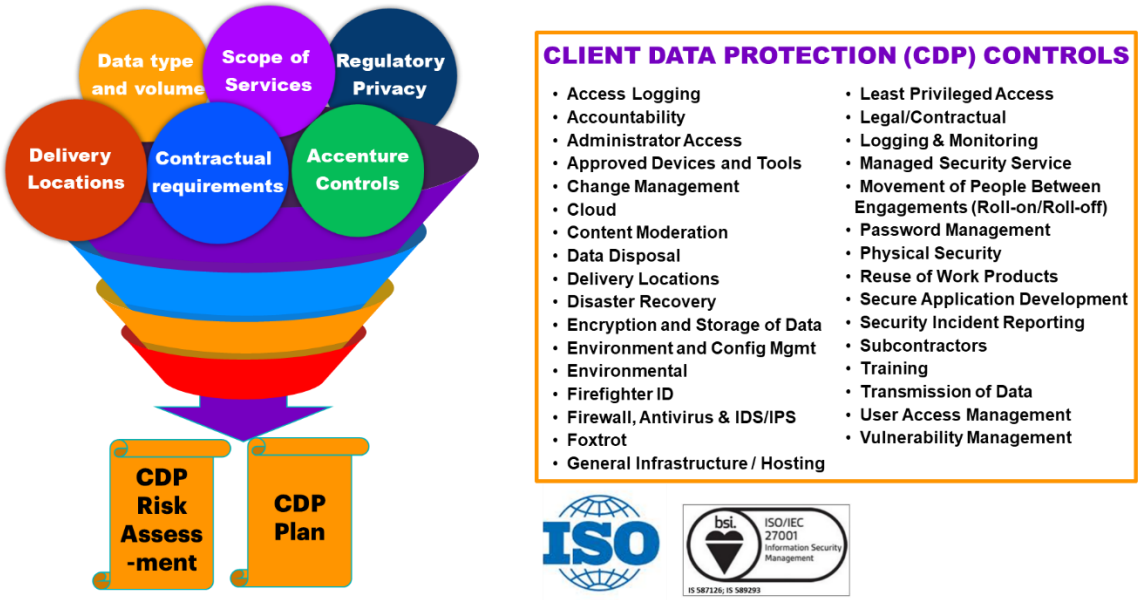


Figura 2 – Sintesi dei requisiti e controlli CDP

1.6. Processo di rilascio

Questa sezione descrive il modello di rilascio al fine di dettagliare i controlli di sicurezza introdotti.

1.7. Branches

Il modello di sviluppo di Pleiade 1 e Pleiade 2 si basa su 3 branch:

- **Master (MM)** - branch principale in cui sono sviluppate le change.
- **Release-candidate (MR)** - branch in cui sono riversate le change e le fix necessarie e legate alla Release da rilasciare.
- **Release (RR)** - rappresenta la release in corso e attualmente in produzione. Su di esso sono mergiate le hotfix legate alle attività di bug fixing.

1.8. Ambienti

- **TestManual - MM/MR/RR** – ambienti in cui viene installato il codice del relativo branch e in cui vengono eseguiti i test manuali.
- **Staging** - ambiente di preview aperto al pubblico (ovvero aperto ai clienti del prodotto), viene usato principalmente per consentire early access a feature sviluppate per i clienti.
- **PreProd** - ambiente configurato, dal punto di vista dell'infrastruttura, come la produzione, in cui sono eseguiti i test di non regressione. Il codice presente sull'ambente di Preprod è quello che viene on demand installato in ambente di Produzione durante il rilascio in una nuova release.
- **Demo** - ambiente aperto ai clienti del prodotto utilizzato per familiarizzazione e simulazioni.
- **Produzione**

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

1.9. Metodologia

La metodologia di sviluppo sicuro di Accenture prevede l'esecuzione attività di analisi statica (SAST) e dinamica a ogni major change delle componenti software sviluppate.

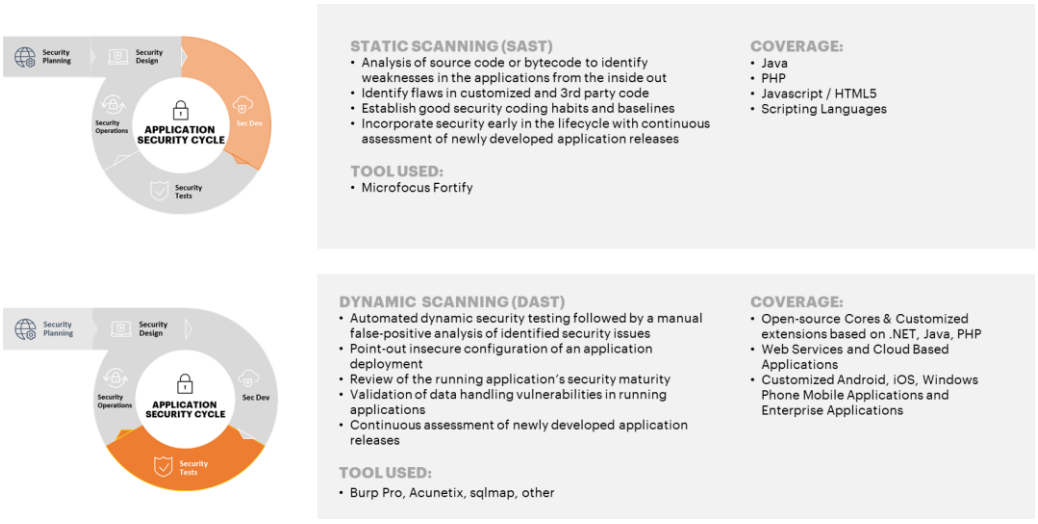


Figura 3 – Differenze tra analisi statica e dinamica

Tali attività verranno eseguite a ogni ciclo di rilascio (major release) di Pleiade 1 e Pleiade 2. Le attività di analisi dinamica verranno inoltre completate da test "manuali" (WAPT).

Di seguito, le principali attività relative al processo di rilascio delle major release di Pleiade 1 e Pleiade 2:

1. Al rilascio della **release-candidate** viene avviato, parallelamente ai test funzionali in ambiente MM e MR, un ciclo di:
    a. **Analisi statica del codice (SAST)**
    b. Condivisione dei risultati con il team di sviluppo e valutazione delle remediation da applicare: correttive software/hardening per tutte le vulnerabilità a severity critica/alta oppure WAF sulle vulnerabilità meno gravi su componenti in end-of-life (Pleiade 1)
    c. Applicazione delle correttive da parte del team di sviluppo e test di non-regression
    d. Condivisione con il team security Accenture e verifica formale delle correzioni applicate
    e. Approvazione o revisione delle correzioni
2. Al rilascio della release in ambiente di **PreProd** viene avviato un ciclo di:
    a. **Analisi dinamica e Web Application Penetration Test (DAST / WAPT)**

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

b. Condivisione dei risultati con il team di sviluppo e valutazione delle remediation da applicare: correttive software/hardening per tutte le vulnerabilità a severity critica/alta oppure WAF sulle vulnerabilità meno gravi su componenti in end-of-life (Pleiade 1)
c. Applicazione delle correttive da parte del team di sviluppo e test di non-regression
d. Condivisione con il team security Accenture delle correzioni applicate
e. Retest delle correzioni da parte del team security Accenture
f. Approvazione o revisione delle correzioni

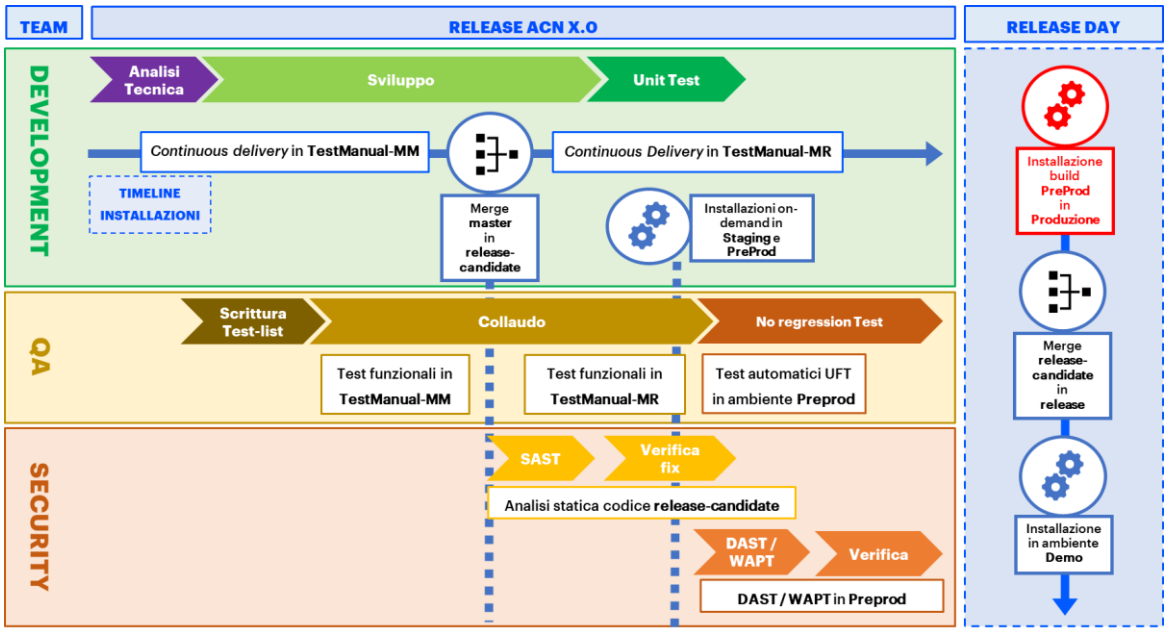


Figura 4 - Nuovo processo di rilascio di Pleiade

3. A valle delle 2 attività precedenti verrà condiviso con i gruppi coinvolti un report di sintesi delle vulnerabilità riscontrate e delle remediation applicate.

4. Oltre alla procedura sopra riportata è da considerare che con cadenza settimanale si procede ad un allineamento con il Global allo scopo di mettere a piano e fixare eventuali criticità segnalate, a titolo di esempio sono state condotte analisi in emergenza sulle vulnerabilità Log4j e SpringBoot.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

1.10. Data Processing Agreement

Più nel dettaglio, ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, viene predisposta la nomina del Responsabile del trattamento, per le attività connesse alla fornitura del servizio che comportano il trattamento di dati personali. Tale nomina avrà validità per il tempo necessario ad eseguire le operazioni e si considera revocata al termine delle operazioni stesse o qualora venga meno il rapporto contrattuale. Accenture presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali e, all'interno del DPA verranno dettagliate le tipologie di dati trattati per le finalità del trattamento esclusivamente riconducibili all'espletamento delle operazioni.

Nell'esercizio delle proprie funzioni, attraverso la sottoscrizione del DPA, il Responsabile si impegna a:

- rispettare la normativa vigente in materia di trattamento dei dati personali;
- trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
- trattare i dati conformemente alle istruzioni impartite dal Titolare, che il Responsabile si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali; inoltre, nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Responsabile deve informare immediatamente il Titolare;
- garantire la riservatezza dei dati personali trattati e verificare che le persone autorizzate a trattare i dati personali:
  - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale di segretezza;
  - ricevano la formazione necessaria in materia di protezione dei dati personali;
  - trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;
- adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (*privacy by design*), nonché adottare misure tecniche ed organizzative adeguate a garantire che i dati personali siano trattati, in ossequio

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (*privacy by default*);

- valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;
- su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;
- ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive e salve le eccezioni previste dal comma 5 del medesimo articolo, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il già menzionato Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

  Si precisa che tale obbligo non si applica alle imprese e organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, o includa il trattamento di dati sensibili;
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE;
- l) nominare gli autorizzati che svolgono le funzioni di "amministratore di sistema", ai sensi dei provvedimenti del Garante italiano per la protezione dei dati personali del 27/11/2008 e del 25/6/2009, conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e comunicandone al titolare l'elenco nominativo con i relativi ambiti di operatività.

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento mette in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre:

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

- la cifratura dei dati personali;
- la pseudonimizzazione e la crittografia dei dati personali;
- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Responsabile del trattamento potrebbe avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento.

Nel caso in cui l'Appaltatore/Responsabile ricorra a subappaltatori o subcontraenti è obbligato a nominare tali operatori a loro volta sub-Responsabili del trattamento e comunicare l'avvenuta nomina al Titolare.

Il sub-Responsabile del trattamento rispetterà obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportati in uno specifico contratto o atto di nomina. Spetta al Responsabile del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. Qualora il sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità.

Inoltre, il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

Il Responsabile comunica al Titolare il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali dell'Appaltatore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.

Al termine della prestazione dei servizi, il Responsabile su richiesta del Titolare, si impegna a:

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

- restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati;
- distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.

Il Responsabile si impegna a attuare quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema".

Il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati siano precisi, corretti e aggiornati nel corso della durata del trattamento – anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati -eseguito dal Responsabile, o da un sub-Responsabile.

Il Responsabile non potrà trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.

Infine, il Responsabile assiste il Titolare al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.

1.11. Corporate Records and Information Management

La Policy 1413 - Corporate Records and Information Management mira a descrivere le modalità in cui la Società gestisce i suoi Corporate Records e dunque i documenti aziendali elettronici e cartacei identificati in Records Retention Schedules per varie funzioni aziendali.

Più nel dettaglio, vengono individuati, gestiti e smaltiti i Documenti Aziendali ai sensi dei Records Retention Schedules per ciascuna Funzione Aziendale. I periodi di conservazione nel Retention Schedule riflettono le leggi, i regolamenti e le buone pratiche commerciali applicabili. Si segnala, che i periodi di conservazione potrebbero variare in base alle previsioni contrattuali e/o normative.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Le registrazioni devono essere smaltite in conformità con i Record Retention Maximums identificati nelle Corporate Function Records Retention Schedule. Se per una categoria non è stato individuato alcun valore massimo di conservazione delle registrazioni, le registrazioni devono essere smaltite entro un anno dal superamento del valore minimo di conservazione delle registrazioni.

Le funzioni aziendali includono:

- Business Performance
- CIO Organization
- Finanza
- Servizi geografici
- Capitale umano e diversità
- Risorse umane
- Legale
- Marketing & Comunicazioni
- Qualità
- Strategy & Corporate Development

Le Corporate Functions sono responsabili delle attività di:

- Sviluppo e mantenimento di piani di conservazione dei record completi in conformità con gli standard e le linee guida di Accenture Records and Information Management (ARIM).
- Creazione di archivi adeguati perla gestione dei Corporate Records in conformità con gli standard e le linee guida ARIM.
- Sviluppo di procedure per supportare e rendere operativi i piani di conservazione dei record in conformità con gli standard e le linee guida ARIM.
- Eliminazione dei record come indicato da Records Retention Schedule.

Accenture Records and Information Management è responsabile delle attività di:

- Sviluppo di standard e linee guida per le pianificazioni di conservazione dei record, le procedure e i repository.
- Fornire supporto e competenza in materia alle Corporate Functions.

Il team Legal e Tax è responsabili per l'attività di:

- Revisione dei periodi di conservazione nei piani in conformità ai requisiti normativi.

1.12. System Security

La Policy 0056- System Security mira a fornire una serie completa di requisiti tecnici di sicurezza per proteggere le informazioni riservate di Accenture, del cliente e di altre terze parti.

La Policy si applica a tutto il personale che partecipa alla progettazione, sviluppo, test e/ o funzionamento di applicazioni, hardware, reti o altri sistemi tecnologici. Il personale che gestisce i

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

progetti e/o le operazioni sui Sistemi è responsabile dell'osservanza della stessa relativamente alle rispettive aree di responsabilità.

La suddetta policy si applica ai Sistemi come descritto di seguito:

- **Accenture Systems**: se non diversamente specificato, si applica alla sicurezza di tutti i Sistemi Accenture e concerne i seguenti principi di sicurezza:
  - identificazione (ad esempio, ID utente) e autenticazione (ad es. password e/o PIN);
  - Autorizzazione (ad esempio, ruoli di accesso e controllo degli accessi);
  - riservatezza (ad esempio, crittografia), integrità (compresi il sistema, l'integrità dei dati e dei messaggi, ad es. accuratezza dell'archiviazione e della trasmissione dei dati) e disponibilità (ad es. accessibile quando necessario);
  - Responsabilità (ad esempio, monitoraggio e audit).

- **Sistemi client**: riguarda tutti i sistemi costruiti o gestiti per i clienti indipendentemente dalla posizione di hosting, e devono essere progettati, costruiti e gestiti in conformità con la Policy 56, Policy 1431 - Data Management e i requisiti relativi al Client Data Protection (CDP).

I dati classificati come altamente riservati o limitati (in base agli standard di classificazione e protezione dei dati) non devono essere tracciati o registrati in log e dovrà essere richiesta una valutazione relativa alla sicurezza per qualsiasi applicazione che contiene dati altamente riservati o riservati.

Gli sviluppatori devono seguire gli standard di codifica e le linee guida di test definite per il sistema in modo da soddisfare i requisiti di sicurezza delle applicazioni e il codice sorgente deve essere protetto in modo da impedire l'accesso non autorizzato.

Gli strumenti di controllo automatico delle fonti devono essere utilizzati per garantire l'affidabilità delle applicazioni e dei dati sviluppati utilizzati nell'applicazione. Questo software deve tenere traccia di tutte le versioni, compresi i commenti di modifica, se necessario.

In merito all'identificazione e alla gestione degli accessi, le password utilizzate dai Sistemi (ad esempio tramite codice applicativo o Tool) devono essere protette (ad esempio, hash o crittografate) e/o l'accesso a qualsiasi file di configurazione contenente password deve essere limitato solo a coloro che hanno bisogno di accesso per eseguire le attività di propria competenza. L'accesso dell'utente, inoltre, sarà registrato e comprenderà tutti gli utenti e gli amministratori.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Le applicazioni devono essere conformi allo standard di sicurezza delle applicazioni Accenture prima di essere introdotte in un ambiente di produzione e saranno testate, in particolare sotto il profilo Security.

I Test sono creati ed eseguiti per convalidare l'efficace funzionamento dei controlli di sicurezza individuati nei documenti di progettazione e gli ambienti di sviluppo, test e produzione saranno separati per ridurre il rischio di accessi non autorizzati o modifiche al Sistema di produzione.

I dati di produzione non devono essere utilizzati in ambienti di sviluppo o di prova senza esplicita approvazione scritta e istruzioni del Data Governor. Se un cliente richiede ad Accenture di utilizzare i dati di produzione del cliente in ambienti non di produzione, il team di progetto deve includere adeguati controlli e ottenere l'approvazione scritta del cliente per accettazione del rischio.

Ove possibile, tali dati dovrebbero essere mascherati e/o resi anonimi, in conformità alla Policy 1431- Gestione dei dati e agli Standards relativi alla Classificazione e Protezione dei dati.

Vulnerability, penetration and integrity test devono essere condotti secondo quanto stabilito dal piano di sicurezza e/o dal piano di protezione dei dati del cliente. In conformità a quanto previsto in tema di Security Assessments e Gestione delle vulnerabilità.

Relativamente ai prodotti e servizi di terze parti, se un'applicazione è concessa in licenza da un fornitore o è sviluppata da un terzo, il capo progetto sviluppa i requisiti di Security come se l'applicazione fosse un'applicazione sviluppata internamente e saranno osservati i requisiti come parte del processo di selezione e contrattazione. Qualora il prodotto di terzi non soddisfi tali requisiti, potrà essere richiesta un'eccezione (seguendo il relativo processo) e se la stessa non viene approvata, l'applicazione non può essere utilizzata.

1.13. Eliminazione della documentazione precedentemente inviata o archiviata dai sistemi di esportazione

Se concordato con il Cliente, il Fornitore potrebbe conservare alcuni dati anche dopo la cessazione del rapporto in funzione del tempo necessario per la gestione di specifici adempimenti contrattuali o di legge, nonché per finalità di natura amministrativa, fiscale e/o contributiva, per il periodo di tempo imposto da leggi e da regolamenti in vigore.

Infine, a conclusione delle attività consistenti nelle finalità di ritenzione dei dati, si provvederà all'erase definitivo degli stessi, in ottemperanza a quanto previsto dalla normativa GDPR.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Tale operazione verrà effettuata al termine dell'eventuale periodo di conservazione derivante da obblighi contrattuali e/o di Legge.

2. Misure di sicurezza in caso di accesso non autorizzato

In questo paragrafo viene riportato il dettaglio delle procedure da utilizzare in caso di accesso non autorizzato e, in particolare, il processo di *Cyber Incident Reporting*. Quest'ultimo è relativo alle segnalazioni di Incidenti ad ASOC e precede l'avviso al Cliente impattato nelle modalità e tempistiche concordate all'interno dei Data Processing Agreement (DPA).

2.1. Cyber incident response

Accenture garantisce un programma di segnalazione di incidenti di sicurezza, indagini e escalation per la risoluzione degli stessi.

In particolare, i dipendenti di Accenture sono tenuti a segnalare effettivi o sospetti incidenti di sicurezza all'Accenture Security Operations Center (ASOC) attivo 24 ore su 24.

Gli eventi segnalati sono esaminati e trasferiti a Team appropriati per ulteriori indagini e analisi da parte di ASOC.

Infatti, Accenture garantisce i propri team relativi a informatica forense, indagini infrastrutturali, cyber threat intelligence, indagini aziendali e team di Data Security legali, ma potrebbe coinvolgere anche esperti esterni in queste aree, se necessario.

Qualora i dati personali siano stati interessati da un incidente, il team legale di Data Privacy supporta per procedere alla notifica dello stesso.

Questi team sono dotati di personale a livello globale per rispondere tutto il giorno a qualsiasi evento di sicurezza.

Se un evento viene identificato come il risultato di un incidente di sicurezza segnalabile, i team aziendali interessati lavorano con i team legali e di comunicazione interna per segnalare prontamente e lavorare in collaborazione con il cliente.

Accenture conduce simulazioni dei suoi protocolli di risposta agli incidenti. Attraverso questi frequenti esercizi Accenture identifica eventuali gap e rafforza le procedure di sicurezza. Queste sono simulazioni realistiche di ipotetici incidenti di sicurezza (ad esempio, malware su larga scala o attacchi ransomware, ecc.) Queste simulazioni sono progettate per simulare eventi effettivi

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

realisticamente, garantendo che i team che rispondono siano soggetti alle stesse incognite che potrebbero incontrare in eventi di sicurezza reali.

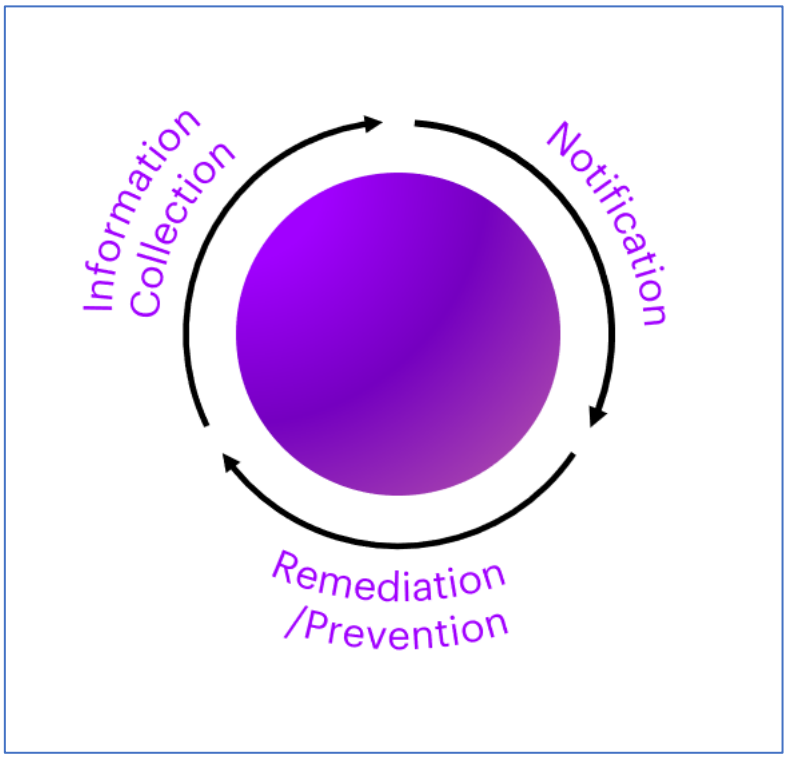


Figura 5

In particolare, il processo di Cyber Incident Response si origina con la segnalazione di un Incidente, segnalato dal dipendente o, in alcuni casi, identificato dal cliente o da una terza parte.

La violazione della sicurezza viene, di conseguenza, segnalata immediatamente presso l'ASOC (Accenture Security Operations Center) che assegnerà il caso e allerterà il Global Asset Protection (GAP) o il Cyber Incident Response Team (CIRT) in base al tipo di incidente.

Questi ultimi, successivamente, svolgeranno un'attività di raccolta preliminare dei fatti e, a seconda di quanto risulta:

- Il GAP / CIRT provvederanno a chiudere il caso;
- Il GAP / CIRT avvisano il Team Legal/ Data Privacy se dati personali o altri dati sensibili sono impattati;
- Il Director del GAP / Client data protection Lead allerta il Crisis Management Committee.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Negli ultimi due casi, verrà interessato l'**Incident Response Team** che si occupa di attività di approfondito fact-finding e di risposta agli incidenti.

Quest'ultimo, in particolare, valuterà l'obbligo di notifica a seguito dell'esame dei dati interessati e delle circostanze specifiche per determinare se Accenture ha l'obbligo di notificarli. Nel dettaglio, nell'ipotesi di obbligo legale, contrattuale o in presenza di eventuali altre ragioni di notifica al Titolare dei dati, il Team Legal e Data Privacy supportano le attività ai fine dell'adempimento degli obblighi legali di notifica.

Nell'ipotesi in cui siano interessati i dati personali dei clienti, Accenture adempie ai propri obblighi legali informando il Titolare (per tali finalità, la parte che ha messo i dati a disposizione di Accenture).

Si segnala che il Titolare dei dati potrebbe essere tenuto a notificare l'incidente ai soggetti interessati o alle autorità di regolazione. Accenture non avrà un ruolo attivo nel prendere tale decisione, ma può fornire al cliente il supporto per l'esecuzione della notifica.

Nella fase successiva verranno adottate immediate misure di mitigazione. Nello specifico, il Client MD (sotto la direzione del Incident Response Team) avvia le fasi di mitigazione per la risoluzione dei problemi (ad esempio, risolvere problemi immediati).

Al contempo, vengono isolate e valutate le aree impattate (ad esempio, fisico, software) in modo tale da circoscrivere la problematica. Successivamente si procede alla:

- Pianificazione di piena remediation: il Client MD avvia attività complete di remediation/ prevenzione (ad esempio, analisi delle cause alla radice) per impedire che l'incidente si riproponga. In seguito, si provvederà ad implementare la remediation ed il Client Team documenta le attività di risoluzione, condividendo l'approccio con il Cliente.
- Valutazione della Compliance: il Client Data Protection fornisce consulenza su controlli aggiuntivi e migliori pratiche ed eventualmente si procede ad eseguire il supporto (se necessario) all'esecuzione da parte del proprietario dei dati degli obblighi legali di notifica.

Una volta completato l'iter sopra descritto, il Client team finalizza la documentazione dell'incidente, incluso il client "sign off", in modo tale da considerare ultimate le attività di Remediation.

Di seguito uno schema riepilogativo del Cyber Incident Reporting Guide:

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

1 SEGNALAZIONE INCIDENT

Chiama ASOC direttamente o invia un modulo tramite pagina web per segnalare un incidente di sicurezza che possa impattare te, Accenture o i nostri clienti

2 CASO ASSEGNATO

ASOC esamina la richiesta e assegna il tuo caso a Global Asset Protection (GAP) o Cyber Incident Response Team (CIRT) in base al tipo di incidente

3 RACCOLTA FATTI

Il GAP / CIRT conduce una raccolta di fatti preliminari e vi contatterà per ulteriori informazioni via telefono, e-mail o Microsoft Teams.

Le indagini in genere impiegano 2-3 ore, ma potrebbero richiedere diversi giorni a seconda del tipo di incidente e della complessità

4 SUPPORTO RICHIESTO

GAP / CIRT richiede supporto aggiuntivo (ad es. Legale, Data Privacy, Crisis Management Committee) se sono necessarie ulteriori indagini

5 ESCALATION DELL'INCIDENT

Se l'incidente richiede un'escalation, Accenture Leadership, i nostri clienti e/o Organismi esterni di regolazione saranno contattati se richiesto.

Ogni situazione di escalation è prevista per legge e obblighi contrattuali.

I clienti ricevono una notifica entro 48 ore dalla segnalazione dell' incidente (GDPR)

6 MIGLIORAMENTI CONSIDERATI

I dati raccolti sono utilizzati da Accenture per migliorare continuamente il programma CDP per garantire che le giuste misure di sicurezza siano implementate

Figura 6

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

3. Tempistiche e modalità di gestione e comunicazione di eventuali violazioni dei dati

Tempistiche e modalità di gestione e comunicazione di eventuali violazioni dei dati (cd. Data Breach) che spetteranno al responsabile del Trattamento ai sensi della normativa vigente, sono dettagliate all'interno dei Data Processing Agreement (DPA) o delle previsioni contrattuali e, pertanto, saranno concordate con il Cliente finale. A titolo esemplificativo si riporta uno stralcio della su citata documentazione per quanto in questa sede di interesse:

f) Assiste il Titolare nel garantire il rispetto degli obblighi inerenti la sicurezza del trattamento, la notifica e la comunicazione dei **Data Breach**, l'effettuazione delle valutazioni d'impatto e la consultazione preventiva, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.
Il Responsabile dovrà adottare ogni cura per comunicare al Titolare del Trattamento senza ingiustificato ritardo e ed entro 12 ore dall'avvenuta conoscenza della violazione dei dati personali ogni informazione di cui venga a conoscenza relativamente a violazioni o potenziali violazioni dei dati personali, contattando a tal fine il Titolare. La notifica deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

I dati forniti da che utilizza il Servizio saranno conservati dall'Appaltatore nel data center in Rozzano (MI), nonche nelle sedi dell'Appaltatore situate a Napoli e Milano. Nel caso in cui l'Appaltatore utilizzi Soluzioni Cloud di Terzi, l'Appaltatore si impegna ad informare circa la sede del fornitore ed i luoghi in cui quest'ultimo potrà procedere all'eventuale trattamento dei dati di . Resta inteso che le soluzioni Cloud di Terzi utilizzate dall'Appaltatore dovranno essere conformi a quanto previsto nel successivo Art. 23.
In caso di un incidente che possa ragionevolmente compromettere la sicurezza o la privacy (data breach) dei dati del l'Appaltatore si impegna ad informare entro 36 (trentasei) ore dalla conoscenza di tale incidente, o nel termine più breve richiesto dalla legge applicabile.

7.5: Pronta notifica
Che informerà senza ingiustificato ritardo di:

- **Violazione dei dati** (*data breach*) - qualsiasi violazione dei dati personali, della quale verrà a conoscenza, entro 36 ore dal momento in cui ne avrà notizia e comunque senza ingiustificato ritardo, fornendo gli elementi utili a valutare l'entità della violazione (es. categorie di dati, categorie e numero approssimativo degli interessati coinvolti);
- **Richieste da parte degli interessati** - qualsiasi richiesta ricevuta direttamente dagli interessati della quale verrà a conoscenza entro 5 giorni lavorativi dal momento in cui ne avrà notizia e comunque senza ingiustificato ritardo;
- **Istruzioni in violazione** - qualsiasi istruzione scritta ricevuta da che, secondo il parere di Accenture, è in violazione della Normativa DP e / o in violazione dei doveri contrattuali ai sensi del presente ADP.

Figura 7

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Più nel dettaglio, il Responsabile informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. Data Breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile e/o di suoi sub-Responsabili.

Inoltre, il Responsabile avvisa tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate per conto del Cliente.

4. Strumenti per monitorare i livelli di sicurezza dei dati

Gli strumenti predisposti al fine di monitorare i livelli di sicurezza dei dati si inquadrano nell'ambito degli Encryption Security Standard e alle procedure di Risk Management.

Con riferimento al primo aspetto, i su citati Standards mirano a fornire ulteriori informazioni dettagliate necessarie in modo tale da essere compliant con la Policy 56 - Sicurezza del sistema, Policy 57 - Uso consentito di informazioni, dispositivi e tecnologia e, infine, la Policy 1431 – Data Management.

Questo standard evidenzia l'assegnazione, l'implementazione, la manutenzione, il monitoraggio e l'applicazione di controlli di crittografia appropriati.

4.1. Security Risk Management

Il rischio di azioni malevole e accidentali all'interno degli ambienti Accenture non può essere completamente eliminato. A tal proposito, il team mantiene alta l'attenzione dei controlli di gestione del rischio, policy, processi e metriche implementate in tutta l'azienda al fine di stabilire le aspettative, misurare i risultati e guidare il cambiamento per:

- stabilire le responsabilità top-down, le priorità e la protezione delle risorse critiche;
- focalizzarsi sulle persone, sui processi e le tecnologie legati alla sicurezza;
- garantire che le best practices siano distribuite ovunque con coerenza.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

4.2. Contesto tecnologico

Accenture genera ogni giorno miliardi di dati e trasmette le informazioni attraverso le reti, le piattaforme e i sistemi. Mantenere l'infrastruttura e i dati sicuri, consentendo ai dipendenti l'adeguata flessibilità, è una sfida continua, soprattutto per Accenture vista come entità globale.

L'Infrastruttura centrale di Accenture ha oltre 350 data center e sedi di hosting, sedi con più di 20.000 server e dispositivi di rete.

Accenture Security Operation Center (ASOC) utilizza alcune delle più avanzate tecnologie di sicurezza per monitorare e rilevare le minacce dell'azienda, e a sua volta aiuta ad implementare soluzioni affidabili. Con questo costante approccio alla fortificazione, Accenture ha guadagnato reputazione positiva per i risk services erogati a terze parti. In particolare, i principali cyber security benchmarking vendor: Security Scorecard, UpGuard e BitSight, riconoscono Accenture tra le società più avanzate nella difesa contro le minacce.

4.3. Descrizione dei controlli di sicurezza implementati per Pleiade

Nei successivi paragrafi verranno descritti i controlli di sicurezza perimetrali ed end-point implementati per la piattaforma Pleiade. In particolare, sarà descritta l'architettura di rete ad alto livello di FW e IPS, WAF, EDR e del vulnerability management.

4.4. Architettura di Rete High Level FW – IPS

Per la realizzazione dell'infrastruttura ci si è affidati all'utilizzo di Next Generation FireWall Fortigate 200E. I NGFW Fortinet soddisfano le esigenze prestazionali di architetture IT ibride altamente scalabili, consentendo di ridurre la complessità e allo stesso tempo gestire i rischi per la sicurezza. Inoltre, consolidano le funzionalità di sicurezza come il sistema di prevenzione delle intrusioni (IPS), il Web filtering, SSL inspection (Secure Socket Layer) e la protezione automatica delle minacce.

Ad alto livello, la rete di AFAST nel nuovo data center è divisa in quattro macroaree ognuna delle quali fa riferimento ad un contesto firewall virtuale. I contesti virtuali sono collegati tra loro dai cosiddetti Intervdom-Link.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

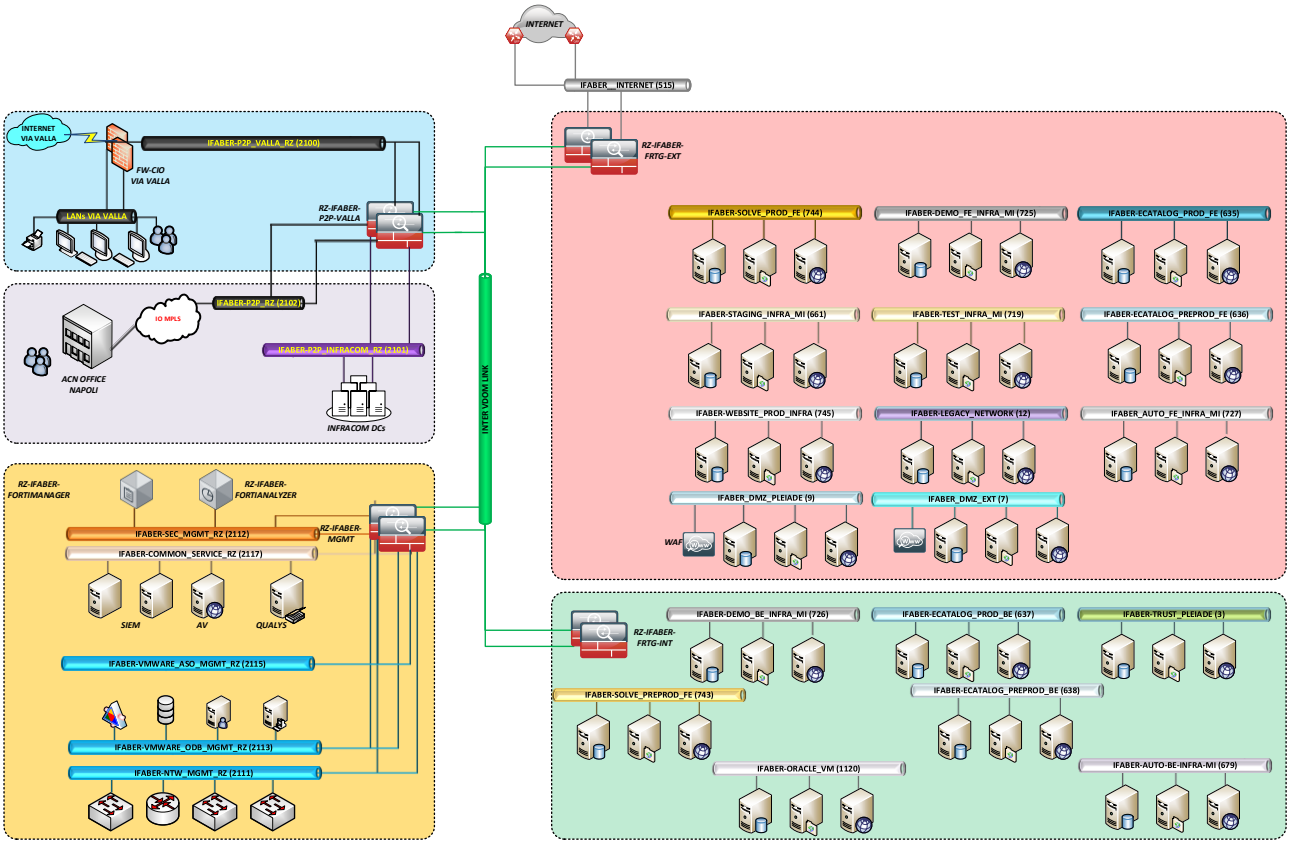


Figura 8- Architettura di Management del firewall del DC primario di Rozzano

- **RZ-IFABER-FRTG-EXT:** contesto firewall virtuale sul quale viene terminata la connettività Internet e le VPN di tipo Site-to-Site e Client-to-Site. Questo contesto ha il compito di effettuare il NAT tra gli IP pubblici e privati mediante i quali sono pubblicati i servizi fruibili da internet. Questo contesto firewall è anche il gateway per tutte le DMZ e le reti di Front-end esposte su internet.
- **RZ-IFABER-FRTG-INT:** contesto firewall virtuale sul quale sono attestate le reti di back-end di AFAST le quali non sono direttamente raggiungibili da internet.
- **RZ-IFABER-FRTG-P2P-VALLA:** contesto firewall virtuale sul quale è attestata la connettività verso la sede di Via Valla (sede AFAST), verso Infracom e verso la DMZ privata di Accenture IO.
- **RZ-IFABER-FRTG-MGMT (root):** contesto virtuale sul quale sono attestate le reti di in band management e le reti di tipo Common Services.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

È stato scelto di adottare l'architettura con il doppio bastione per rispettare le best practice di sicurezza e fornire un doppio strato Firewall ed IPS di protezione al back-end. Inoltre, la segregazione degli ambienti consente di creare set di policy chiare e facilmente mantenibili.

All'interno delle quattro macroaree definite in precedenza sono configurate le VLAN dove vengono attestati i servizi.

La stessa configurazione è stata replicata sul DC secondario di Padova.

Sul sito primario i due firewall sono ridondati tra loro mediante una connessione diretta di alta affidabilità. L'HA è di tipo attivo-attivo, ovvero le connessioni, le tabelle di routing ed i NAT sono replicati in real-time dalla macchina primaria su quella di standby. In questo modo, in caso di switch tra le due appliance non c'è perdita della sessione ed il risultato è una user experience migliorata in quanto l'utente finale non percepisce lo switch tra i firewall.

Per ottimizzare la gestione dell'infrastruttura è utilizzata la console FortiManager, una console di gestione centralizzata per i device Fortinet, che include inoltre funzioni di dashboarding per visualizzare lo stato degli apparati.

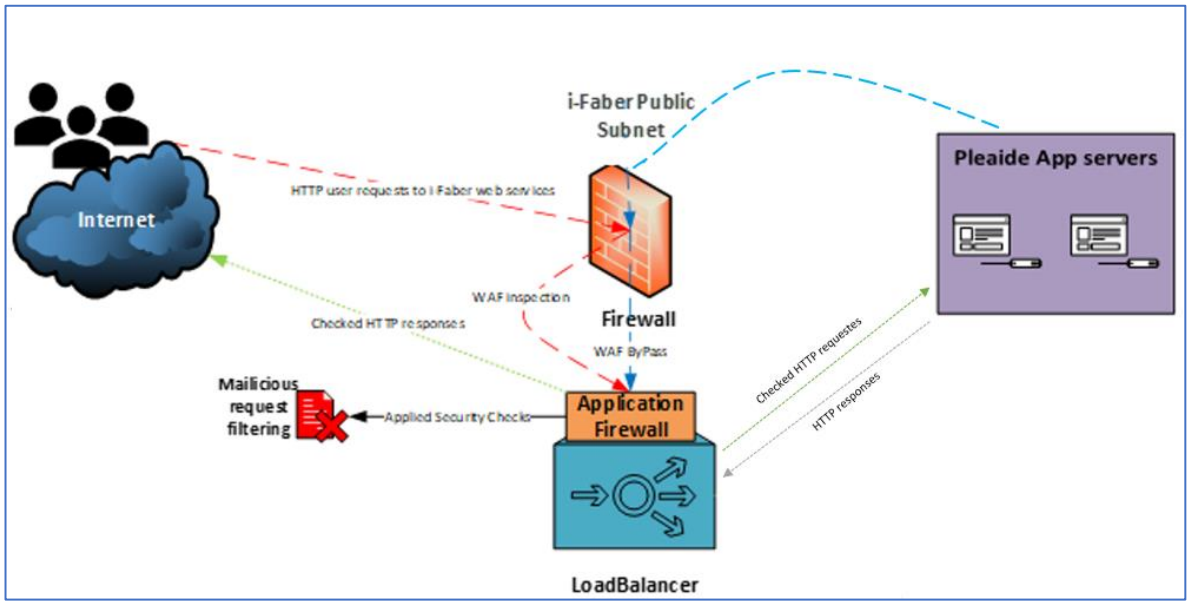
La management console del Fortigate 200E è una Virtual machine installata a Rozzano e configurata in alta affidabilità con una VM gemella installata a Padova. La VM di Rozzano avrà ruolo di master nell'alta affidabilità.

Figura 9 -Schema di ridondanza console di management

4.5. Web Application Firewall

Il Web Application Firewall (WAF) protegge le applicazioni Web da una varietà di attacchi a livello applicativo come cross-site scripting (XSS), SQL injection, cookie poisoning, XML injection, Remote Command Execution, Remote File Inclusion, ecc.

Rispetto ai sistemi di rilevamento delle intrusioni (IDS / IPS), i WAF hanno forte attenzione al traffico delle applicazioni e sono in grado di fornire un'analisi approfondita del flusso di dati.



Il Web Application Firewall che protegge le applicazioni AFAST in particolar modo l'applicazione Pleiade, è un modulo incluso nei bilanciatori Citrix ADC che espongono su Internet le applicazioni.

Figura 10

Le interazioni applicative che provengono da internet, attraverso il Firewall AFAST arrivano sul Web Application Firewall che provvede ad ispezionare il traffico per verificarne il contenuto. Il WAF, attraverso opportune policies e controlli di sicurezza, gestisce il traffico in ingresso differenziando le interazioni malevole da quelle legittime ed applicando, sulla base della configurazione del flusso applicativo protetto, le relative misure di sicurezza.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

4.6. End point Detection & Response: Tanium

Tanium è una soluzione largamente diffusa per proteggere e gestire gli endpoint aziendali. L'architettura linear-chain brevettata da Tanium fa sì che tutte le attività di security ed operation che in precedenza venivano effettuate in diverse ore di lavoro vengano eseguite in pochi secondi. Offre la possibilità di eseguire query su workstation e server, nonché eseguire script e distribuire patch.

L'EDR rileva, reagisce ed effettua un rapido recovery dell'infrastruttura in caso di attacchi e di interruzioni dell'attività.

Se una workstation è coinvolta in un incidente di sicurezza per infezione da malware, la pulizia del host può essere eseguita in maniera automatizzata.

L'Incident Response Team può installare funzionalità aggiuntive sulle workstation coinvolte in un incidente per analizzare i dati e confermare che non è avvenuto un data leak.

4.7. Vulnerability Management e Server Configuration Compliance: Qualys

Qualys Vulnerability Management è un servizio basato su cloud che offre una visione globale dei sistemi potenzialmente vulnerabili e identifica le soluzioni al fine di garantirne la protezione. Aiuta a identificare le minacce e monitorare cambiamenti non attesi in rete prima che si trasformino in violazioni. È conosciuto per rapida implementazione, precisione e scalabilità impareggiabili, nonché per la vasta integrazione con altri sistemi aziendali. Consente inoltre la revisione dei processi interni.

La capacità di Qualys di tracciare i dati delle vulnerabilità degli host consente di utilizzare i report in modo interattivo per comprendere meglio la sicurezza della rete. Fa uso di una libreria di report integrata che consente di essere customizzata senza necessità di ripetere la scansione. I report possono essere generati su richiesta o automatizzati per poi essere condivisi in PDF o CSV.

Il processo di gestione delle vulnerabilità prevede scansioni sul perimetro Esterno (IP pubblici) e Interno (IP privati):

- Esterno: prevede delle scansioni settimanali del perimetro.
- Internal: sono generalmente eseguite due volte al mese oppure possono essere on-going, ovvero eseguite con agent qualys che forniscono scansioni ogni quattro ore.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

Un altro aspetto fondamentale è la compliance. La compliance è il processo di validazione che assicura che le configurazioni in essere rispettino gli standard di sicurezza delineati per i server. Questa viene costantemente monitorata attraverso gli agent Qualys ed eventuali deviazioni delle configurazioni dei sistemi rispetto agli standard Accenture vengono gestite con lo stesso processo di Vulnerability Management.

4.8. Gestione della sicurezza

Il team Accenture MSS è responsabile per la gestione delle infrastrutture di sicurezza FW/IPS e WAF e per il monitoraggio continuo dei tentativi di intrusione attraverso una piattaforma di raccolta e correlazione degli eventi di sicurezza (SIEM Splunk). I potenziali incidenti di sicurezza vengono monitorati, analizzati e gestiti da un team che opera in H24 dal Cyber Fusion Center di Napoli.

La soluzione Tanium è gestita e monitorata dal Cyber Security Incident Response Team (CSIRT) globale di Accenture.

5. Modalità di restrizione all'accesso ai dati

Nel presente paragrafo sono dettagliate le modalità attraverso cui è possibile predisporre restrizioni all'accesso dei dati. Le suddette modalità, che potrebbero essere concordate all'interno dei DPA, e dunque di concerto con il Cliente, attengono ai seguenti profili:

- Sicurezza Applicativa;
- Sicurezza infrastrutturale;
- Sicurezza Fisica.

Sotto il primo aspetto, nello specifico, è possibile predisporre la profilazione degli accessi in base al ruolo, l'utilizzo di credenziali uninominali, l'autenticazione delle utenze attraverso Username/Password e l'utilizzo di password sicure.

Inoltre, è possibile garantire la mascheratura della base dati, l'Encryption degli stessi e la tracciatura degli accessi. Si precisa, in ogni caso, che vengono implementati meccanismi di protezione dei dati estratti, validazione dei dati in input e protezione delle comunicazioni Client/Server.

Con riferimento alla sicurezza infrastrutturale, anche sotto tale profilo è garantita la profilazione degli accessi in base al ruolo, l'utilizzo di credenziali uninominali, l'autenticazione delle utenze

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

attraverso Username/Password e l'utilizzo di password sicure. Inoltre, sono implementati meccanismi di protezione da Malware Signature Based, Protezione/Cifratura delle linee di comunicazione, isolamento della rete da altri sistemi e protezione del traffico tramite IDS/IPS.

Sarà, in aggiunta, prevista l'attivazione di restrizioni di accesso sul File System, un programma di protezione dischi rimuovibili e, infine, la soluzione di Disaster Recovery.

Per quanto attiene, invece, alla Sicurezza fisica, viene garantita la limitazione di accesso ai locali deputati al trattamento, la profilazione degli accessi in base al ruolo, l'utilizzo di Tessere di Accesso uninominali e la limitazione di accesso agli Archivi cartacei. Si segnala, inoltre, la presenza di sistemi antieffrazione, di video-sorveglianza locali e si garantisce l'eventuale movimentazione dei materiali in modalità sicura.

Infine, sarà cura di Accenture designare per iscritto e individualmente (ed aggiornare periodicamente), in conformità a quanto previsto dalla normativa in materia di Amministratori di Sistema e come concordato all'interno del DPA, i soggetti incaricati della gestione e della manutenzione degli impianti di elaborazione dei dati. Sarà dunque redatto un documento contente gli estremi identificativi delle persone fisiche preposte, con relativo elenco delle funzioni attribuite e, con cadenza almeno annuale, sarà verificato l'operato delle stesse in modo tale da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalla normativa vigente.

Saranno, inoltre, svolte attività di formazione e controllo e saranno adottati sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione ed archivi elettronici da parte degli Amministratori di Sistema.

6. Eventuali coperture assicurative in relazione al rischio privacy

Le coperture assicurative inerenti al rischio Privacy possono essere considerate "Project Based", pertanto, non sono predisposte a livello Corporate. Più nel dettaglio, infatti, occorre distinguere tra clausole in tema di Liability previste contrattualmente e, dunque, concordate con il Cliente che possono arrivare ad un massimale fino a tre volte l'importo del contratto o, in alternativa, è possibile, ove richiesto dal Cliente, predisporre una protezione assicurativa ad hoc.

Accenture Financial Advanced
Solutions & Technology S.r.l.
Via Privata Nino Bonnet, 10 | 20154 Milano
Tel: +39 02 7775 1111
Pec: accenturefast@legalmail.it

In particolare, a titolo esemplificativo, è possibile predisporre polizze assicurative la cui copertura includa la cyber liability e in merito alla Responsabilità professionale di Accenture per sinistro relativo a network security and privacy liability nella fornitura dei servizi oggetto del contratto per:

a) accesso non autorizzato o uso non autorizzato di un sistema informatico o di una rete;
b) denial of service attacks;
c) ricezione o trasmissione di codice malevolo;
d) mancata protezione di dati riservati, informazioni personali o aziendali;
e) raccolta illecita di informazioni riservate, informazioni personali o aziendali;
f) violazione delle leggi sulla privacy, statuti, regolamenti in relazione a un evento descritto in (d) o (e).