IT - Policy di gestione e conservazione dei dati di proprietà dei clienti

In questo documento vengono illustrate le policy e le procedure che utilizza 4Science per la conservazione e la gestione dei dati di proprietà dei clienti, durante il periodo di servizio.

Modalità in cui i dati vengono conservati ed eventualmente archiviati

I dati presenti all'interno degli applicativi che mette a disposizione 4Science sono sempre salvati in cloud, su Amazon Web Services (AWS, https://aws.amazon.com), a meno di esplicita indicazione concordata nel contratto. In quest'ultimo caso sono definite separatamente anche le procedure di eliminazione.
I suddetti dati possono essere contenuti in:

- Tabelle di Database AWS RDS (es.: Postgresql e Mysql) o analogo (es.: DynamoDB, Redshift, etc.);
- Bucket AWS S3, o Glacier;
- Volumi EBS di AWS EC2;

Nello specifico per i seguenti servizi Saas:

- **Servizi Saas Dataverse e Saas DSpace** (GLAM e CRIS):
  1. I materiali digitali caricati, accessibili solo da Dataverse e DSpace tramite policy impostate sugli stessi e dal server applicativo, sono salvati su Bucket S3;
  2. Tutti i file sono sottoposti a versioning e le versioni così prodotte sono mantenute per 30gg;
  3. I file dell'applicativo sono sempre conservati su volumi EBS dedicati in uso esclusivo al cliente, accessibili solo dal server applicativo;
  4. Sono presenti backup giornalieri mantenuti per 14gg monitorati con procedura automatica;
  5. Esiste un database riservato ad ogni cliente (su cluster condiviso) su Amazon RDS i cui dati sono accessibili solo tramite applicativo e da personale autorizzato 4Science;
  6. Vengono effettuati backup giornalieri anche per i database e conservati per 15gg;
  7. I log degli applicativi vengono costantemente elaborati in modo da renderli anonimi. Vengono, inoltre, spostati in un'area centralizzata per conservazione (30gg) e analisi sull'utilizzo del servizio.

- **Servizi SaaS OJS**:
  1. I file dell'applicativo ed i materiali digitali caricati sono conservati su volumi EBS dedicati in uso esclusivo al cliente, accessibili solo dal server applicativo;
  2. Sono presenti backup giornalieri mantenuti per 15gg monitorati con procedura automatica;
  3. Esiste un database riservato ad ogni cliente (su cluster condiviso) su Amazon RDS i cui dati sono accessibili solo tramite applicativo e da personale autorizzato 4Science;
  4. Vengono effettuati backup giornalieri anche per i database e conservati per 15gg;
  5. I log degli applicativi vengono costantemente elaborati in modo da renderli anonimi. Vengono, inoltre, spostati in un'area centralizzata per conservazione (30gg) e analisi sull'utilizzo del servizio.

Misure di sicurezza predisposte in caso di accesso non autorizzato

Per prevenire accessi non autorizzati vengono utilizzati ruoli AWS IAM e chiavi RSA personali per l'accesso ai server. Il solo ruolo di supporto tecnico può accedere ai dati per verificare eventuali richieste di assistenza.

1. Ogni macchina possiede un log degli accessi utilizzabile per un'indagine iniziale;
2. AWS GuardDuty è attivo sull'intero account AWS. É un servizio di monitoraggio continuo della sicurezza che analizza ed elabora le seguenti fonti di dati: Log VPC, log di eventi AWS CloudTrail e log DNS. Utilizza i feed delle informazioni sulle minacce, come gli elenchi di IP e dominii dannosi, e Machine learning per identificare attività inaspettate e potenzialmente non autorizzate/dannose all'interno dell'ambiente AWS;
3. 4Science programma periodici Application Penetration test e Network Penetration test (sia dall'interno che dall'esterno della rete) per garantire la sicurezza dell'infrastruttura.

Presenza di strumenti per monitorare i livelli di sicurezza dei dati

La sicurezza del dato è garantita tramite versioning su S3 e backup su EBS. In aggiunta è in essere una Procedura di verifica annuale dei backup. Per DSpace in particolare i dati vengono monitorati tramite procedura automatica per la verifica della consistenza tra i Bucket S3 e l'hash precedentemente salvato su database.

Lo staff tecnico di 4Science ha accesso completo ai dati per poter erogare i servizi concordati con il cliente. É inoltre possibile, tramite i vari applicativi, definire il livello di accesso esterno ai dati utilizzando funzionalità specifiche.

Tutti i servizi sottoposti a questa qualifica raccolgono informazioni di natura pubblica, le singole istituzioni possono decidere quali informazioni raccogliere esplicitando i termini di utilizzo e le richieste di autorizzazione.
Per quanto riguarda il trattamento di eventuali dati non pubblici, vengono stabiliti e configurati in fase di setup dell'applicativo.

Nello specifico per i seguenti servizi Saas:

- **SaaS Dataverse**: É possibile definire quali utenti/gruppi hanno accesso ai metadati ed i file di uno specifico dataset o collezione (Dataverse) di dataset.

- **SaaS DSpace** (GLAM e CRIS): L'istituzione può decidere quali metadati sono visibili ai soli amministratori e se i metadati di specifici item devono essere visibili solo a determinati gruppi di utenti o dopo un determinato periodo (embargo). La medesima restrizione di accesso può essere applicata individualmente ai singoli file allegati agli oggetti: pubblici, embargo, visibili esclusivamente a specifici utenti/gruppi. I dati sono modificabili dai singoli utenti che li creano solo allo stato di bozza, una volta pubblicati possono essere modificati solo da gruppi di amministratori definiti dall'ente.

- **SaaS OJS**: Le proposte/pubblicazioni approvate, hanno per loro definizione una natura pubblica. Un'eventuale restrizione di accesso può essere definita dal cliente per motivi commerciali (vendita abbonamenti/accessi).

Le proposte di sottomissione sono visibili oltre che dagli autori stessi dal comitato di redazione in base al workflow definito dalla singola rivista e secondo le politiche di accesso ai dati, sempre da loro definite ed esplicitate nelle apposite pagine della rivista (es.: revisione in forma anonima delle proposte, elenco pubblico/chiuso o aperto di revisori, etc.).

Tempistiche e modalità con cui vengono gestite e comunicate le eventuali violazioni dei dati

- *Se vi è un data breach interno* (se la violazione avviene internamente all'impresa, quindi sui dati che 4Science tratta direttamente): In questo caso il soggetto autorizzato deve dare tempestiva comunicazione per scritto al titolare del trattamento, descrivendo anche ciò che ha rilevato, la tipologia di breach e la quantità di dati coinvolti, le circostanze in cui il breach si è verificato e di come ne è venuto a conoscenza e le azioni da lui adottate al fine di limitare i danni o interrompere il breach. L'avviso è, quindi, tempestivo, avviene non appena l'autorizzato scopre la violazione. Il titolare poi comunica al Garante, qualora ne ricorrano i presupposti, entro 72 ore dal momento in cui è venuto a conoscenza della violazione.
- *Se vi è un data breach esterno* (se la violazione avviene su dati di cui noi siamo titolari, ma sono affidati ad un responsabile esterno): Il responsabile esterno del trattamento è obbligato a comunicare tempestivamente e senza ingiustificato ritardo (non più tardi di 12 ore) la violazione al titolare del trattamento, sia tramite e-mail che tramite pec.

Coperture assicurative in relazione al rischio privacy

La Società è munita di assicurazione R.C. Professionale "Rischi Diversi" che comprende, in particolare:
- "L'assicurazione si obbliga a tenere indenne 4Science S.r.l. di quanto questi sia tenuto a risarcire quale civilmente obbligato ai sensi di legge, a titolo di risarcimento del danno cagionato a terzi in conseguenza dell'attività professionale esercitata. Quest'ultima è relativa alla fornitura di soluzioni integrate nel campo dell' IT, nell'offerta di soluzioni, prodotti e/o servizi di sicurezza, di integrazione e di centralizzazione delle applicazioni; nonché nell'offerta di prodotti consulenziali nell'area dello sviluppo software, nella fornitura di servizi e di consulenza per l' e-commerce, il datawarehouse e per la realizzazione di applicazioni internet.
- L'assicurazione non copre specificatamente i danni derivanti da cyber crime, ma una polizza specifica all'uopo è in corso di valutazione e sottoscrizione".