Esercizio 2: prodotto per il Corso

CyberSecurity and Data privacy, UNIFI, DISIT Lab

Autore: Paolo Nesi, paolo.nesi@unifi.it

L'azienda PROV45 (come data Processor) sta acquisendo dati amministrativi del negozio MODAnuova per inviarli anonimizzati a Snap4City tramite connessione HTTPS verso un Orion Broker autenticato con certificato. I dati potranno essere acquisiti in due modalità: (1) andando a prenderli dal loro gestore amministrativo con una connessione autenticata, per anonimizzarli ed in seguito inviarli a Snap4City; (2) fornendo la possibilità di caricare un file di dati amministrativi anonimizzati che sarà a sua volta inviato a Snap4City. Snap4City (come data Processor) riceve dati solo in forma anonima ed è GDPR compliant. I dati finali saranno processati per fornire informazioni statistiche al negozio MODAnuova.

Si declina ogni responsabilità per omissioni ed inesattezze, è solo un esempio didattico.

BOZZA DI DPIA

Data Protection Impact Assessment (DPIA) per il trattamento di dati amministrativi del negozio MODAnuova

1. Contesto e descrizione del trattamento

Il negozio MODAnuova intende utilizzare il servizio di PROV45 (in qualità di data processor) per l'invio di dati amministrativi anonimizzati alla piattaforma Snap4City (anch'essa data processor). I dati verranno utilizzati esclusivamente per produrre informazioni statistiche a beneficio del negozio stesso.

Modalità di acquisizione e trasferimento dei dati:

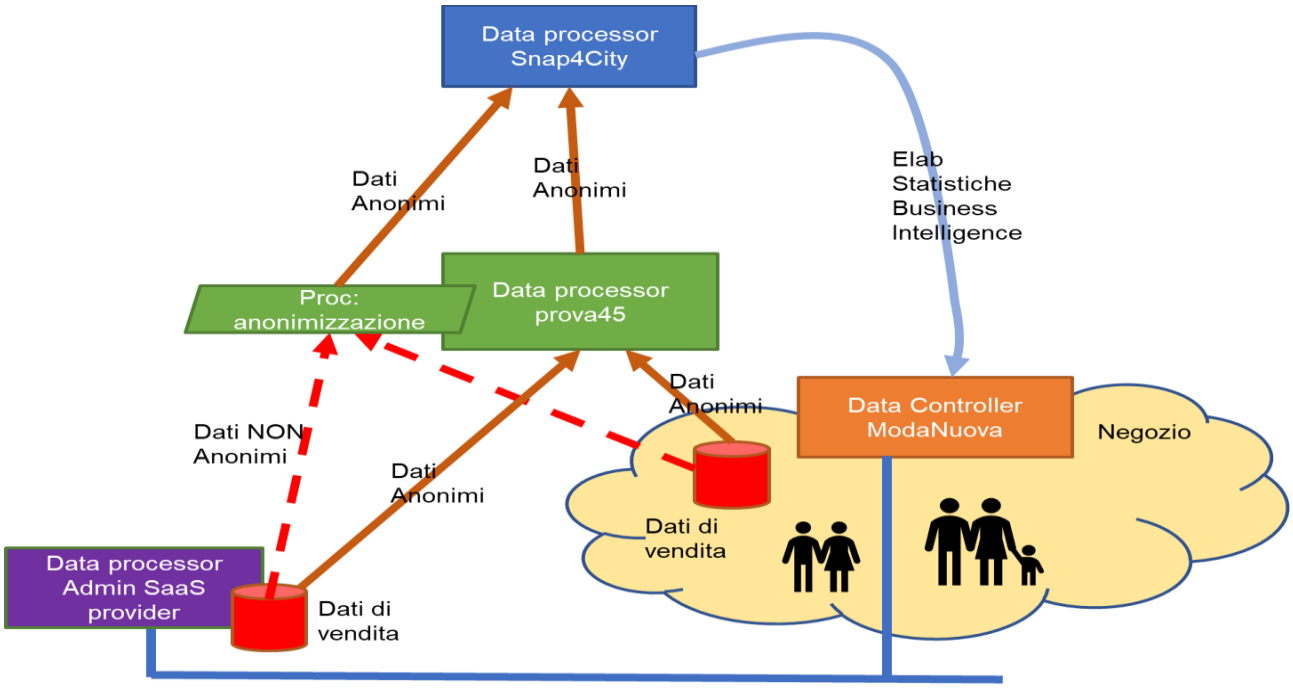
- Modalità 1: PROV45 recupera i dati dal sistema gestionale amministrativo del negozio, attraverso connessione autenticata. I dati vengono anonimizzati prima dell'invio a Snap4City.
- Modalità 2: MODAnuova carica un file contenente dati amministrativi già anonimizzati, che PROV45 invia a Snap4City.

Trasferimento a Snap4City:

- I dati vengono inviati via HTTPS a un Orion Broker autenticato con certificato.
- Snap4City riceve solo dati già anonimizzati.

Finalità:

- Generazione di statistiche di supporto alle decisioni aziendali di MODAnuova.
- Nessuna finalità di profilazione individuale o marketing.



2. Valutazione della necessità e proporzionalità

- Finalità legittima del titolare: ottenere analisi statistiche sui dati amministrativi.
- Limitazione della finalità: i dati saranno usati solo per le statistiche interne.
- Minimizzazione dei dati: solo dati necessari e anonimizzati sono trasferiti a Snap4City.
- Pseudonimizzazione/anonimizzazione: PROV45 effettua anonimizzazione prima della trasmissione.

3. Valutazione dei rischi per i diritti e le libertà degli interessati

- Rischio principale: perdita di confidenzialità dei dati amministrativi in fase di acquisizione o prima dell'anonimizzazione.
- Livello di rischio post-mitigazione: basso.
- I dati in forma identificabile non lasciano l'ambiente controllato di PROV45.

4. Misure di mitigazione previste

☑ Connessione sicura (HTTPS con certificato) per tutte le trasmissioni di dati.
☑ Accesso autenticato ai sistemi gestionali di MODAnuova.
☑ Anonimizzazione robusta effettuata da PROV45.
☑ PROV45 tiene il dato privato solo il tempo necessario al processing e non lo storicizza.
☑ Nessun trasferimento di dati personali a Snap4City: solo dati già anonimizzati.
☑ Contratti di nomina a responsabile del trattamento (art. 28 GDPR) tra MODAnuova e PROV45, e tra MODAnuova e Snap4City.
☑ Audit periodico delle procedure di anonimizzazione.
☑ Registrazione delle operazioni di accesso ed elaborazione: al dato di MODAnuova, etc..

I processi di PROVA45 non sono accesibili da internet e nmon da terzi se non autorizzati. E comunque l'accesso viene loggato.

5. Conclusioni della valutazione

- Il rischio residuo per i diritti degli interessati risulta basso grazie alle misure adottate.
- Il trattamento rispetta i principi del GDPR (liceità, correttezza, trasparenza, minimizzazione, integrità e riservatezza).
- Non è richiesto il consulto preventivo del Garante ai sensi dell'art. 36 GDPR.

6. Allegati (facoltativi)

- contratto di nomina a responsabile (art. 28).
- Policy di anonimizzazione di PROV45.
- Schema tecnico dell'architettura di connessione.

7. Dichiarazione del Titolare / DPO

Il presente DPIA è stato redatto per attestare la conformità del trattamento descritto al GDPR e in particolare all'art. 35.
Dopo esame delle modalità operative e delle misure di sicurezza, si ritiene che il rischio residuo per i diritti e le libertà degli interessati sia basso e adeguatamente mitigato.

Firma del DPO di MODAnuova:

Nome:
Data:

Policy di Anonimizzazione dei Dati

Versione 1.0 – [data]
Organizzazione: PROV45

1. Scopo

Questa policy definisce le modalità operative e le misure di sicurezza che PROV45 applica per l'anonimizzazione dei dati amministrativi acquisiti dal negozio MODAnuova, prima dell'invio alla piattaforma Snap4City.

Obiettivo: garantire che i dati trasmessi a Snap4City non contengano informazioni personali identificabili, in conformità al GDPR (artt. 5, 25, 32, considerando 26).

2. Ambito di applicazione

- Tutti i dati amministrativi acquisiti da MODAnuova per il servizio di generazione statistiche.
- Tutti i sistemi e i processi di PROV45 coinvolti nel trattamento, inclusi accesso, trasformazione, memorizzazione temporanea e trasmissione.
- Tutto il personale PROV45 coinvolto nelle attività di elaborazione.

3. Principi generali

☑ Minimizzazione dei dati: acquisire solo le informazioni strettamente necessarie.
☑ Anonimizzazione robusta: eliminare qualunque dato personale identificabile.
☑ Sicurezza by design e by default: integrare la protezione dei dati in tutte le fasi del trattamento.
☑ Auditabilità: garantire tracciabilità e verifica delle operazioni di anonimizzazione.

4. Processo di anonimizzazione

4.1 Acquisizione dei dati

- Connessione autenticata e cifrata (HTTPS con certificato).
- Log degli accessi.
- Autorizzazione controllata (ruoli definiti).
- Dati admin acquisiti daily

4.2 Identificazione dei campi sensibili

- Identificatori diretti (es. nome cliente, codice fiscale, indirizzo, CAP) individuati come dati da rimuovere.
- Identificatori indiretti (es. ID cliente, codice interno) valutati e rimossi o aggregati.
- Dati numerici o di vendita privi di riferimenti personali conservati per le statistiche.

4.3 Trasformazione / eliminazione

- Rimozione completa dei campi contenenti dati personali.
- Generalizzazione o aggregazione di eventuali campi che potrebbero contenere dati a rischio di re-identificazione.
- Verifica di output: test periodici per escludere rischio di re-identificazione.

4.4 Salvataggio temporaneo

- Archiviazione intermedia su server cifrati e protetti.
- Conservazione dei dati non anonimizzati limitata al minimo necessario per l'elaborazione (max 24 ore).
- Cancellazione sicura (wipe) dei dati identificabili dopo l'anonimizzazione.

4.5 Invio a Snap4City

- Solo dataset già anonimizzato.
- Trasmissione via HTTPS autenticata. Qos = 2, etc…
- Log dell'operazione sia da PROV45 che da Snap4City

5. Misure di sicurezza tecniche e organizzative

☑ Accesso controllato e tracciato ai sistemi.
☑ Connessioni cifrate TLS/HTTPS.
☑ Autenticazione a più fattori per il personale tecnico.
☑ Audit periodici delle procedure di anonimizzazione.
☑ Formazione specifica del personale sui principi di privacy e sicurezza.
☑ Contratti di riservatezza firmati dal personale autorizzato.

6. Responsabilità

- Il **Responsabile della Protezione Dati (DPO)** di PROV45 supervisiona l'applicazione di questa policy.
- Il **Responsabile tecnico del trattamento** è incaricato di implementare le procedure operative.
- Tutto il personale coinvolto è tenuto a rispettare questa policy.

7. Revisione e aggiornamento

Questa policy viene riesaminata almeno annualmente o ogni volta che:

- cambiano i sistemi o i processi di trattamento;
- vengono identificate vulnerabilità o non conformità;
- mutano i requisiti legali o contrattuali.

8. Approvazione

Redatto da:
[Nome e Ruolo]

Approvato dal DPO di MODAnuova:
Nome: _____
Firma: _____
Data: _____

Allegati

- Contratto di nomina a responsabile del trattamento (PROV45).
- Contratto/sub-nomina per Snap4City.
- Schema tecnico (architettura di rete).
- Esempio di cartello informativo in negozio.
- Registro dei trattamenti aggiornato.

Registro delle Versioni – Policy di Anonimizzazione di PROV45

Versione	Data	Descrizione modifiche	Approvato da
1.0	[gg/mm/aaaa]	Prima emissione della policy	[Nome / Ruolo]
1.1	[gg/mm/aaaa]	Correzioni minori di forma / stile	[Nome / Ruolo]
1.2	[gg/mm/aaaa]	Aggiornamento processo di anonimizzazione	[Nome / Ruolo]
2.0	[gg/mm/aaaa]	Revisione completa per adeguamento normativo GDPR	[Nome / Ruolo]

- end---