Esercizio 1: 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 installando delle telecamere e dei sensori di conteggio dentro il Negozio MODAnuova. Queste telecamere e sensori prenderanno dei dati che tramite connessione protetta TSL si connetteranno per una elaborazione dentro un BOX installato direttamente dentro il negozio. Il BOX a sua volta processa i dati in tempo reale ed invia i dati in forma anonimizzata in HTTPS verso Snap4City Orion Broker autenticato con certificato. Snap4City (come da processor) riceve dati solo in forma anonima ed è GDPR compliant. I dati finali saranno processati per fornire informazioni statistiche al negozio MODAnuova.
Su questa base andiamo a produrre un DPIA che dovrebbe essere firmato dal DPO del negozio che il proprietario del dato.

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

BOZZA di DPIA – Data Protection Impact Assessment

Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 GDPR

Progetto: Installazione di telecamere e sensori di conteggio in negozio MODAnuova

Versione: 1.0
Data: [Inserire data]

Titolare del trattamento:
MODAnuova S.r.l.
[Indirizzo completo], [Email contatto privacy]

Responsabile della protezione dei dati (DPO):
[Nome e contatto del DPO]

1. Descrizione sistematica del trattamento

Finalità del trattamento:

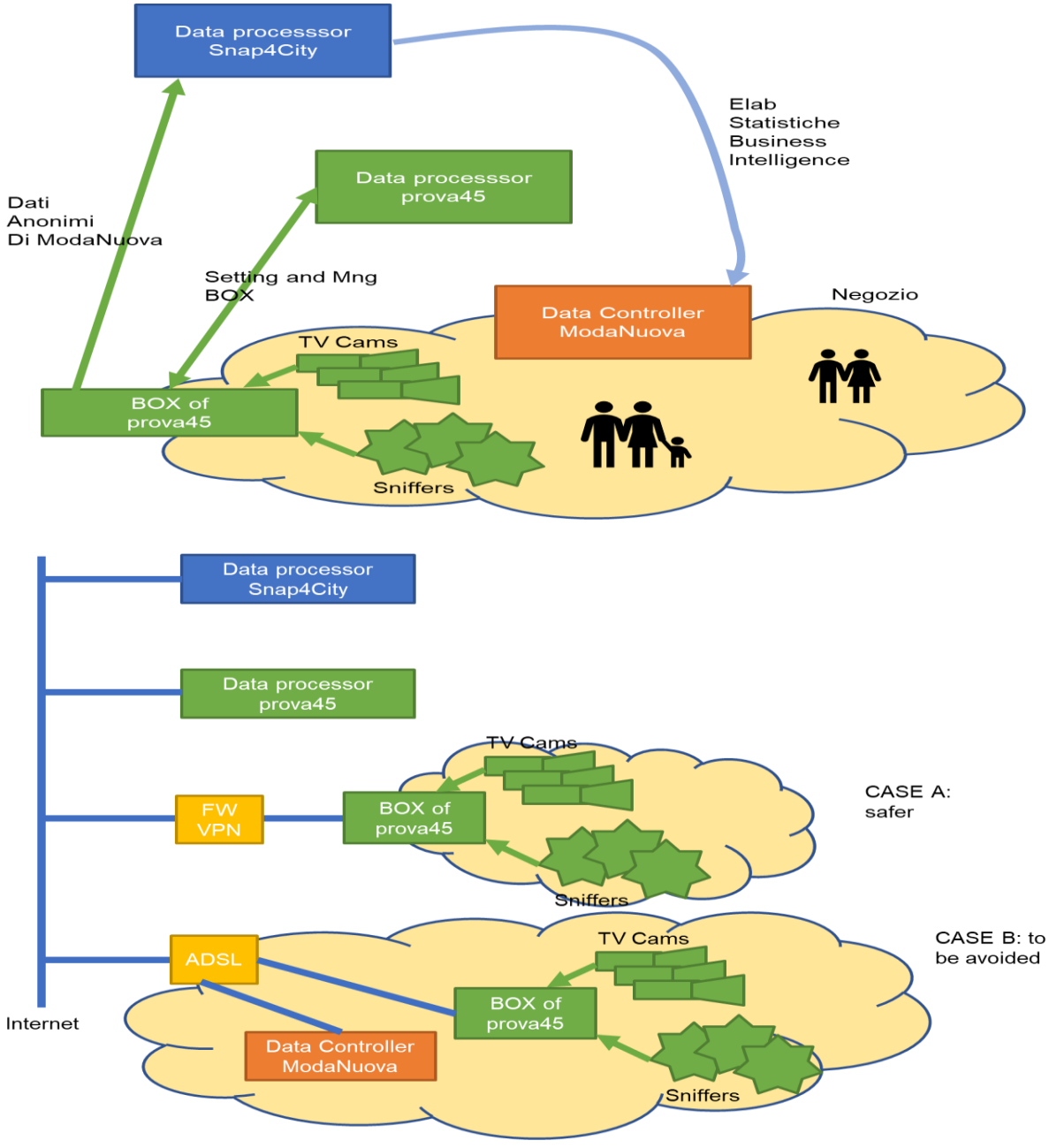
- Conteggio di persone all'interno del negozio.
- Analisi statistica dei flussi e delle presenze per ottimizzare la gestione commerciale.
- Fornitura di reportistica anonima a MODAnuova.

Mezzi di trattamento:

- Telecamere e sensori di conteggio installati nei locali di vendita.
- BOX di elaborazione locale con connessione TSL protetta ai sensori.
- Invio in tempo reale dei soli dati anonimizzati via HTTPS autenticato (con certificato) verso Snap4City Orion Broker.

Flusso dei dati:

1. Sensori e telecamere raccolgono dati grezzi in negozio.
2. Dati trasmessi in modo sicuro (TSL) al BOX locale.
3. BOX elabora i dati in tempo reale, trasformandoli in forma anonima (es. conteggio aggregato, eliminazione/mascheramento di qualunque dato potenzialmente identificativo).
4. Solo i dati anonimizzati vengono inviati via HTTPS autenticato a Snap4City Orion Broker.
5. Snap4City (ulteriore processor) archivia ed elabora esclusivamente dati anonimi per fornire reportistica.



Durata di conservazione:

- Dati grezzi pseudonimizzati (se presenti) sul BOX: cancellazione immediata o entro massimo 24 ore (solo per elaborazione locale).
- Dati anonimi su Snap4City: conservazione per analisi statistiche senza limiti GDPR (non dati personali).

Ruoli e responsabilità:

- MODAnuova: Titolare del trattamento.
- PROV45: Responsabile del trattamento (installazione, gestione BOX, primo livello di elaborazione e anonimizzazione).
- Snap4City: Sub-responsabile del trattamento (ricezione e analisi di dati già anonimizzati).

2. Necessità e proporzionalità

☑ **Necessità:**

- Conteggio visitatori per esigenze di business intelligence e miglioramento servizio.
- Non esistono alternative equivalenti che non trattino alcun dato (conteggio manuale non sostenibile).

☑ **Proporzionalità:**

- Nessuna registrazione identificativa (video di sorveglianza a fini di sicurezza NON inclusa in questo progetto).
- Elaborazione locale dei dati per anonimizzazione prima della trasmissione.
- Dati anonimi inviati al broker di Snap4City, conforme GDPR.
- Obiettivo limitato a statistica aggregata.

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

Rischio identificato	Gravità potenziale	Probabilità	Note
Accesso non autorizzato ai dati grezzi	Medio	Bassa	Limitato al BOX in sede, connessioni protette.
Re-identificazione da dati di conteggio	Molto bassa	Molto bassa	Dati inviati sono già anonimizzati.
Violazione di confidenzialità in trasmissione	Medio	Molto bassa	TSL/HTTPS con certificato.
Uso improprio da parte di fornitori	Medio	Bassa	Contratti di processor/sub-processor GDPR compliant.

Rischio complessivo (prima delle misure): Medio.
Rischio residuo (dopo le misure): Basso.

4. Misure previste per mitigare i rischi

☑ **Tecniche:**

- Criptaggio TSL/HTTPS per tutte le comunicazioni.
- Autenticazione a certificato verso Snap4City.
- Elaborazione locale in BOX con immediata anonimizzazione.
- Cancellazione dati grezzi sul BOX entro max 24 ore.
- Nessuna registrazione video identificabile.
- Vpn
- Separazione della rete del box rispetto a quella del negozio..

☑ **Organizzative:**

- Contratto di data processing con PROV45 che specifica compiti e limiti (Art. 28 GDPR).
- Contratto di sub-processing tra PROV45 e Snap4City conforme GDPR.
- Accesso ai dati locali limitato a tecnici autorizzati.
- Registro dei trattamenti aggiornato.

☑ **Informative agli interessati:**

- Cartelli informativi visibili in negozio.
- Informativa privacy disponibile anche online.
- Indicazione chiara che i dati servono solo a fini statistici, in forma anonima.

☑ **Sicurezza:**

- BOX fisicamente protetto in negozio.
- Aggiornamenti software regolari.
- Logging degli accessi al BOX.
- Pen-test e audit periodici se previsti.

5. Valutazione finale del rischio residuo

Le misure implementate riducono in modo sostanziale il rischio. I dati trasmessi verso Snap4City sono anonimi e non consentono identificazione diretta o indiretta delle persone.
Conclusione: rischio residuo basso.

Non si ritiene necessaria la consultazione preventiva con l'Autorità di controllo (art. 36 GDPR).

6. Conclusione della valutazione

- Il trattamento è lecito (art. 6.1.f GDPR: legittimo interesse).
- Proporzionato e limitato alla finalità dichiarata.
- Conforme ai principi di privacy by design e by default (art. 25 GDPR).
- Misure tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR.

7. Firma e 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.

ESEMPIO DI CARTELLO INFORMATIVO

📷 **Attenzione – Conteggio visitatori in corso**

Per migliorare l'esperienza dei nostri clienti, questo negozio utilizza:
☑ Telecamere di conteggio persone (senza registrazione identificativa)
☑ Sensori di rilevamento dispositivi Wi-Fi/Bluetooth (anonimizzati)

Finalità:

- Analisi statistica e gestione dei flussi di visita
- Ottimizzazione del servizio

Come funziona:

- I dati sono elaborati localmente in tempo reale
- Trasmissione solo di dati anonimi e aggregati verso server certificati e sicuri

Base giuridica:

- Interesse legittimo del Titolare (art. 6.1.f GDPR)

Chi tratta i dati:

- Titolare del trattamento: MODAnuova S.r.l.
- Responsabile del trattamento: PROV45
- Sub-responsabile: Snap4City

Garanzie di protezione:
☑ Nessuna identificazione personale o tracciamento individuale
☑ Cancellazione rapida di eventuali dati grezzi sul posto
☑ Trasmissione cifrata e sicura

Per saperne di più:
Consulta la nostra Privacy Policy su [URL del sito o QR code]
Oppure chiedi informazioni al personale.

Titolare del trattamento:
MODAnuova S.r.l. – [Indirizzo]
Email: [indirizzo email privacy]

Variante breve (formato ridotto per vetrina/ingresso)

📷 **Area monitorata per conteggio visitatori**
Usiamo telecamere/sensori solo per contare presenze in forma anonima.
Nessuna identificazione personale.
Info: [sito/QR] – MODAnuova S.r.l.

MODELLO DI NOMINA A RESPONSABILE DEL TRATTAMENTO

modello di Nomina a Responsabile del Trattamento (art. 28 GDPR) pronto per l'uso tra MODAnuova (Titolare) e PROV45 (Responsabile), personalizzato sullo scenario che hai descritto (installazione e gestione di telecamere/sensori di conteggio con elaborazione locale e invio anonimo a Snap4City).

(Art. 28 Regolamento UE 2016/679 - GDPR)

Tra
MODAnuova S.r.l., con sede legale in [Indirizzo completo], C.F./P.IVA [Dati fiscali], in qualità di **Titolare del Trattamento** (di seguito "Titolare")

E
PROV45 S.r.l., con sede legale in [Indirizzo completo], C.F./P.IVA [Dati fiscali], in qualità di **Responsabile del Trattamento** (di seguito "Responsabile")

Articolo 1 – Oggetto dell'Incarico

Il Titolare nomina il Responsabile per le attività di trattamento relative a:
☑ installazione, configurazione e manutenzione di telecamere e sensori di conteggio presso i punti vendita MODAnuova;
☑ gestione di un BOX locale di elaborazione dei dati raccolti;
☑ anonimizzazione dei dati in tempo reale sul BOX;
☑ trasmissione sicura (HTTPS con certificato) dei soli dati anonimizzati verso Snap4City Orion Broker;
☑ supporto tecnico e monitoraggio del funzionamento del sistema.

Articolo 2 – Natura e finalità del trattamento

☑ **Finalità**: conteggio delle presenze e analisi statistica dei flussi di visitatori per finalità gestionali e commerciali interne.
☑ **Natura dei dati**: dati derivanti dal conteggio persone e da segnali Wi-Fi/Bluetooth dei dispositivi mobili; non sono trattati dati identificativi diretti.
☑ **Categorie di interessati**: clienti e visitatori dei punti vendita.
☑ **Tipo di trattamento**: raccolta tecnica, elaborazione locale, anonimizzazione, trasmissione sicura.

Articolo 3 – Durata dell'incarico

La presente nomina decorre dalla data di sottoscrizione e resta valida per tutta la durata del contratto di fornitura dei servizi sopra descritti.

Articolo 4 – Obblighi del Responsabile

Il Responsabile si impegna a:
- Trattare i dati personali solo su istruzione documentata del Titolare.
- Garantire che le persone autorizzate al trattamento si impegnino alla riservatezza.
- Implementare misure tecniche e organizzative adeguate (art. 32 GDPR) tra cui:

- Trasmissione cifrata (TSL/HTTPS).
- Elaborazione locale con anonimizzazione immediata dei dati.
- Cancellazione di eventuali dati grezzi entro massimo 24 ore.
- Assistere il Titolare nel garantire i diritti degli interessati.
- Collaborare per eventuali valutazioni di impatto (DPIA).
- Mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare la conformità al GDPR.
- Consentire audit o ispezioni ragionevoli da parte del Titolare.
- Non nominare sub-responsabili senza autorizzazione scritta del Titolare.

Articolo 5 – Sub-Responsabili

Il Titolare autorizza l'uso del sub-responsabile:
Snap4City S.r.l. (o altro provider che fornisce il servizio Orion Broker), esclusivamente per la ricezione e gestione dei dati anonimizzati.
Il Responsabile garantirà che ogni sub-responsabile offra garanzie adeguate di conformità al GDPR e stipuli accordo conforme all'art. 28 GDPR.

Articolo 6 – Trasferimenti verso paesi terzi

Il Responsabile non trasferirà dati personali al di fuori dello Spazio Economico Europeo senza preventiva autorizzazione scritta del Titolare e senza garanzie adeguate ai sensi del GDPR.

Articolo 7 – Misure di sicurezza

Il Responsabile adotta e mantiene misure di sicurezza adeguate, tra cui:
☑ Protezione fisica del BOX locale.
☑ Accesso riservato solo a personale autorizzato.

☑ Logging e controllo degli accessi.
☑ Aggiornamenti software/firmware regolari.
☑ Crittografia e autenticazione tramite certificato per la trasmissione dei dati.

Articolo 8 – Riservatezza

Il Responsabile si impegna alla più stretta riservatezza sulle informazioni e sui dati di cui venga a conoscenza nell'esecuzione dell'incarico.

Articolo 9 – Violazioni dei dati personali

Il Responsabile notifica al Titolare eventuali violazioni di dati personali senza ingiustificato ritardo e comunque entro 24 ore dalla scoperta, fornendo tutte le informazioni utili.

Articolo 10 – Termine dell'incarico

Al termine del rapporto contrattuale, il Responsabile si impegna a:
☑ Restituire o cancellare i dati personali eventualmente conservati, secondo istruzioni del Titolare.
☑ Garantire la cancellazione sicura di ogni copia residua.

Articolo 11 – Legge applicabile e foro competente

La presente Nomina è regolata dalla legge italiana e dal GDPR. Foro competente: [indicare foro].

Firma per accettazione

Il Titolare del Trattamento
MODAnuova S.r.l.
Firma: _____
Nome: _____
Ruolo: _____
Data: _____

Il Responsabile del Trattamento
PROV45 S.r.l.
Firma: _____
Nome: _____
Ruolo: _____
Data: _____

■ End --