GIOIELLERIA GATTOPARDO

DI LENNY ARTALE

# ANALISI RISCHI

GIOIELLERIA GATTOPARDO
DI LENNY ARTALE

**ANALISI RISCHI**

# GIOELLERIA GATTOPARDO

L'analisi dei rischi per la privacy è una delle questioni che più ha interessato la Gioelleria Gattopardo di Lenny Artale al fine di predisporre un adeguato Regolamento protezione dei dati.
Per tale motivo si è cercato di affrontarla con metodo, verificando il lavoro della società, evidenziando le criticità ed il modo con il quale vengono affrontate.
Nel dettaglio:
L'art. 32 del Regolamento Generale per la Protezione dei Dati (il cosiddetto GDPR), riportato nel seguito per facilità di consultazione, indica gli obblighi per il titolare e per il responsabile del trattamento, nonché i requisiti necessari per trattare dati personali: " *Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio che comprendono, tra le altre, se del caso:*

- *la pseudonimizzazione e la cifratura dei dati personali;*
- *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
- *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali 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".*

La valutazione di rischio e impatto di un trattamento tiene conto dei diritti e libertà delle persone fisiche, mentre in altri casi, come ad esempio nel campo della sicurezza informatica, la valutazione dei rischi è stata centralizzata sull'organizzazione  e non sugli interessati.
L'analisi svolta non ha riguardato esclusivamente il titolare o la sua organizzazione, ma è stata effettuata nell'ottica degli interessati rispetto ai  in cui sono coinvolti.
Pertanto non si è fatto riferimento esclusivo agli aspetti di sicurezza del trattamento ma anche ai suoi effetti complessivi sugli interessati compreso il grado di innovatività con cui viene effettuato.
Per il calcolo del rischio sono stati tenuti in considerazioni due valori fondamentali:

- Il livello di impatto sugli interessati di un determinato trattamento;

- La probabilità di accadimento di una eventuale minaccia.

Il rischio della minaccia è calcolato sul trattamento mentre il livello di impatto sugli interessati.

La necessità di predisporre una adeguata analisi dei rischi, ci ha indotto a ricercare ed individuare una modalità semplice ed efficace.

Partiremo da una prima valutazione qualitativa del **RISCHIO POTENZIALE LORDO** (cioè una valutazione senza considerare i controlli e le misure di sicurezza applicate).

Per fare questo, abbiamo individuato le tipologie e le quantità dei dati coinvolti nelle diverse attività di trattamento; in base a questi dati, per ogni trattamento, abbiamo poi individuato/definito i rischi potenziali, che potrebbero derivare agli interessati dalla perdita di sicurezza dei dati.


*Didascalia 1 – Procedere quindi a classificare l'impatto per i diritti e le libertà degli interessati in una scala da 1 a 5 (1 = Molto Basso, 5 = Molto Alto) a fronte dell'eventuale mancanza di: Riservatezza, Integrità, Disponibilità, Resilienza, o Altre situazione di rischio.*

*Didascalia 2 – Valutare poi la probabilità di accadimento (in assenza di contromisure e controlli) in base all'ipotetica probabilità/frequenza di accadimento, con la stessa scala di valori, da 1 a 5 (1 = Molto Basso, 5 = Molto Alto)*

**Fatto ciò**, siamo stati in grado di individuare, nel registro dei trattamenti i punti di attenzione su cui focalizzare la nostra analisi e i nostri interventi di sicurezza.

In base alle misure di sicurezza applicate e ai controlli eseguiti nel trattamento, abbiamo cercato di ridurre la probabilità/frequenza di accadimento e/o l'impatto per le varie tipologie di rischio analizzate.

Con la stessa matrice sopra indicata calcoliamo quindi il **rischio effettivo netto** (cioè ridotto dalle contromisure di sicurezza applicate).

La riduzione del livello di rischio, **dal rischio lordo al rischio netto**, rappresenta l'efficacia delle misure di sicurezza applicate e dovrebbe evidenziare gli interventi/investimenti fatti per assicurare la "sicurezza".

Le misure di sicurezza applicate possono essere considerate: **efficaci, effettive, monitorate e controllate periodicamente**, valutate in modo oggettivo, mantenendo le evidenze dell'attività eseguita.

Rating per la classificazione del livello di rischio

Quando la valutazione del "**rischio netto**" nella matrice è: verde (p*i < 7) = livello di rischio considerato accettabile;
giallo ( p*i <11) = **necessario pianificare interventi di mitigazione**;
arancio/rosso (p*i >11) = **indispensabile attivare rapidamente contromisure di adeguamento**.

A questo punto abbiamo individuato soluzioni tecniche e organizzative che consentono di ridurre eventuali rischi elevati e sottoposti all'approvazione del titolare del trattamento dati.
Per ogni soluzione sono stati definiti i tempi di attuazione per consentire la scelta degli interventi in linea con le politiche aziendali.
Nei trattamenti in cui persistono rischi elevati si è proceduto con la valutazione d'impatto sulla protezione dei dati (la cosiddetta **DPIA**, Data Protection Impact Assessment) secondo quanto indicato dal Working Party 29 nel documento n. 248 del 4 ottobre 2017 – Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "***possa presentare un rischio elevato***" ai fini del regolamento (UE) 2016/679.
Sono state, altresì, definite le modalità di accettazione da parte del titolare del trattamento dati di rischi superiori a quelli accettabili attraverso apposite procedure con l'eventuale richiesta d'interpello preventivo all'Autorità di controllo.

Quali misure di sicurezza sono state applicate ai trattamenti?

Per ridurre il rischio nel trattamento dei dati si sono individuate alcune soluzioni applicabili, ad esempio la pseudonimizzazione e la cifratura.
In particolare:
Per le operazioni relative alla **gestione del sistema informatico**, si è concordemente previsto che:

- i *server* applicativi centralizzati siano ospitati in locali dedicati e messi in sicurezza;
- l'accesso ai suddetti locali sia riservato ai soli soggetti autorizzati;
- l'accesso logico ai sistemi informativi sia protetto da *user* ID e *password* utente con scadenza periodica;
- ogni utente disponga di *user* ID e *password* personale per l'accesso ai sistemi informativi della società, custodisca accuratamente le proprie credenziali evitando che terzi soggetti possano venirne a conoscenza e le aggiorni periodicamente secondo le tempistiche imposte dalla Società;
- siano utilizzati esclusivamente *software* di cui si possiede regolare licenza;
- siano effettuate verifiche periodiche in merito all'eventuale installazione di *software* non autorizzati sui sistemi operativi dell'Impresa;
- la rete sia protetta da *firewall* e da *software antivirus/antispam*;
- i *backup* dei dati residenti sui *server* siano salvati periodicamente ed i supporti adeguatamente conservati;
- sia garantita la tracciabilità dei documenti prodotti e delle modifiche a questi apportate;
- la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa.

Per il trattamento di dati con rischi elevati (***dati particolari= sensibili/biometrici/genetici***) è stato necessario alzare il livello di sicurezza e valutare con attenzione la conformità dei processi di gestione degli ***asset*** coinvolti nel trattamento, rispetto alle normative di settore, agli standard internazionali di gestione e controllo (ad esempio: ISO 27001, COBIT ecc.).

**La tabella riporta un elenco non esaustivo delle misure adottate per ridurre i rischi.**
**E'necessario valutare di volta in volta quali misure sono utilizzabili a riduzione dei singoli rischi.**

| tipologia di misura | misura | descrizione/esempi |
|---|---|---|
| controlli di sicurezza funzionali | anonimizzazione | I dati vengono conservati in fascicoli privi di indicazione. |
| controlli di sicurezza funzionali | sicurezza dei documenti cartacei | sono state definite le regole per la conservazione dei documenti cartacei contenenti dati utilizzati durante il trattamento, come debbono essere stampati, archiviati, distrutti e scambiati. |
| controlli di sicurezza funzionali | minimizzazione della quantità dei dati personali | Al fine di ridurre la quantità dei dati acquisiti si è individuato rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, (pdf) ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati |
| controlli di sicurezza fisici | gestione delle postazioni di lavoro | Sono state adottate misure per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accesso, lavoro su uno spazio di rete di backup, controlli di integrità logging etc.). |
| controlli d'organizzazione | Organizzazione privacy | All'interno della Gioielleria di Lenny Artale esiste ed è operativa un'organizzazione in grado di dirigere e controllare la protezione dei dati personali |
| controlli d'organizzazione | Politiche privacy | Il titolare del trattamento dei dati dispone di una banca dati documentale utile per formalizzare gli obiettivi e le regole da applicare nel campo della protezione dei dati (rischi, principi chiave da seguire, obiettivi, regole da applicare, ecc.,) |

| tipologia di misura | misura | descrizione/esempi |
|---|---|---|
| controlli d'organizzazione | Gestire le violazioni dei dati personali | Esiste un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla privacy delle persone interessate (definizione delle responsabilità a piano di reazione, caratterizzazione delle violazioni etc.) |
| controlli d'organizzazione | Gestione del personale ( allo stato inesistente ) | E' operativo, a seguito di più incontri, un piano di formazione in materia di protezione dei dati e procedure/istruzioni che descrivono le istruzioni per l'accesso ai dati . |
| controlli d'organizzazione | Relazioni con terze parti | Esiste una procedura per ridurre i rischi che l'accesso legittimo ai dati da parte di terzi possa porre alle libertà della vita privata delle persone interessate (*identificazione dei terzi, contratto di subappalto, convenzione etc*.) |
| controlli d'organizzazione | supervisione | Esistono delle collaudate misure per fornire una visione globale e aggiornata dello stato di protezione dei dati e conformità con il GDPR |

Sono stati ritenuti indispensabili controlli periodici per poter dichiarare laconformità di gestione rispetto alle esigenze derivanti dal trattamento dei dati e come sempre, mantenere evidenza dell'attività eseguita.

**Il Regolamento Generale per la Protezione dei Dati, predisposto per conto della Gioielleria di Lenny Artale prevede, espressamente:**

- l'aggiornamento del Registro dei trattamenti, la valutazione del rischio per gli interessati;
- la verifica preventiva delle misure di sicurezza applicate al trattamento (Privacy by Design).

Le procedure interne prevedono e stabiliscono verifiche periodiche sui trattamenti eseguiti (privacy by default).

La conservazione da parte del titolare del trattamento delle evidenze dell'attività eseguite, i documenti utilizzati, i piani di adeguamento in corso, rappresentano la documentazione minima di riscontro.