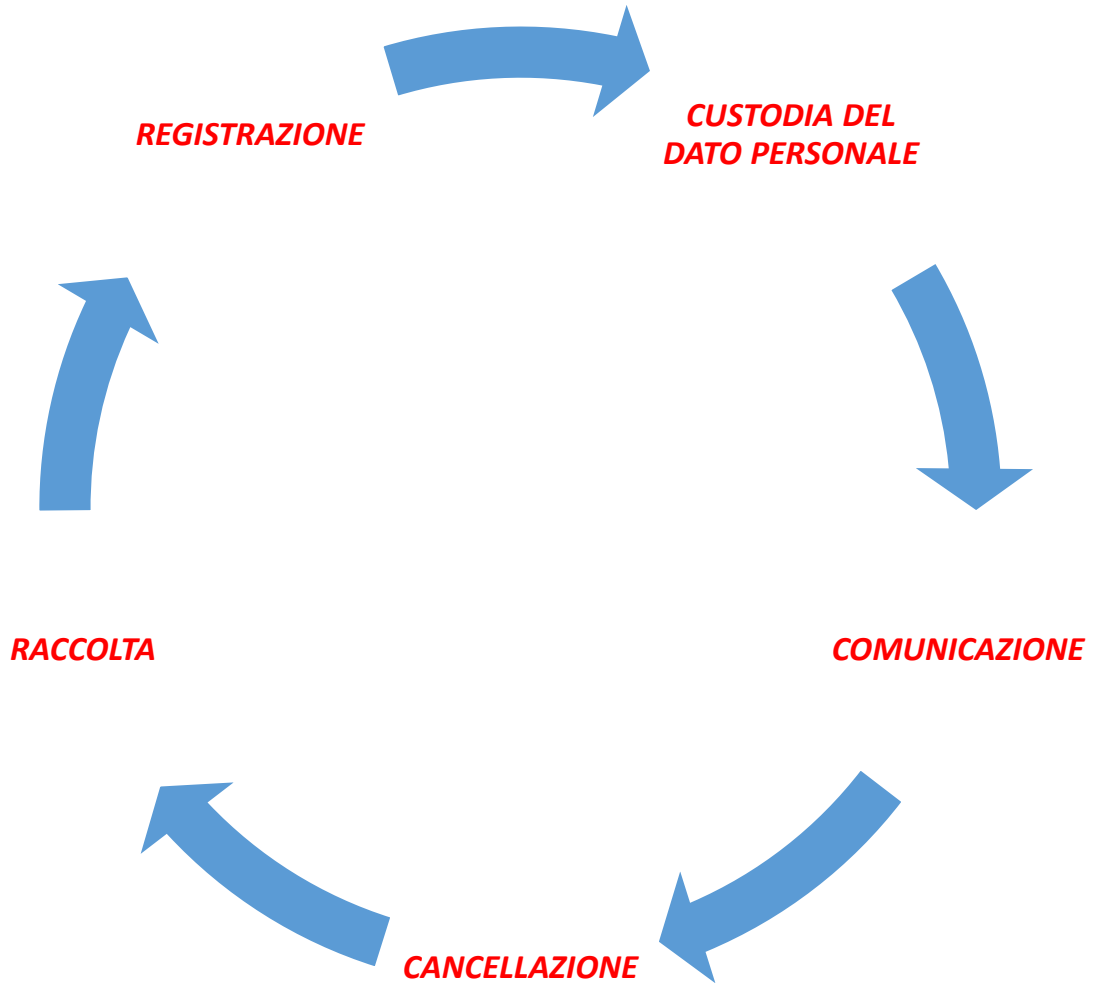
APPROVATO CON DELIBERAZIONE 741 del 03/09/2021

Data	Descrizione	Redatto	Verificato	Approvato
27/05/2021	**Prima emissione**	Dott.ssa Francesca Fasano (DPO)	Dott.ssa Teresa Leggieri (RQA)	Dott. Giovanni Palazzo (DAA)

INDICE DEL DOCUMENTO

1. FASE DEL CICLO DI VITA DEL DATO PERSONALE



2. FONTI LEGISLATIVE

- ✓ Art. 32 del Regolamento Europeo 2016/679
- ✓ Artt.35 e 36 del Regolamento Europeo 2016/679

3. DESTINATARI

- U.O.C. SERVIZI INFORMATIVI AZIENDALI
- U.O.S. AFFARI LEGALI – Ufficio Privacy
- Responsabili del Trattamento
- Amministratori di Sistema

4. PREMESSA

Il Regolamento Europeo chiede alle organizzazioni di stabilire misure IDONEE a tutela e sicurezza delle banche dati. A differenza di quanto precedentemente disposto dal D.Lgs. 196/2003, il Regolamento non stabilisce un elenco di misure minime di sicurezza ma affida alle organizzazioni la responsabilità di identificare opportune cautele in funzione dei propri rischi.

Le misure di sicurezza dunque devono tenere conto:

a. dello stato dell'arte dell'organizzazione;
b. dei costi di attuazione;
c. della natura, oggetto, contesto e finalità di trattamento;
d. della probabilità e gravità del rischio per i diritti e le libertà delle persone fisiche.

Le misure possono essere:

- Tecniche, ovvero riguardare soluzioni fisiche, tecnologiche in grado di intervenire automaticamente sul pericolo;
- Organizzative, ovvero riguardare soluzioni capaci di minimizzare i rischi individuati attraverso l'organizzazione del lavoro.

All'art.32 il Regolamento ci propone **una lista aperta e non esaustiva** ("tra le altre, se del caso") delle misure, affidando comunque all'organizzazione le soluzioni più opportune.
Fra queste si citano:

Pseudonimizzazione e cifratura dei dati

La pseudoanonimizzazione è una tecnica diversa dall'anonimizzazione.
La PSEUDOANONIMIZZAZIONE, infatti, toglie dalle banche dati tutti i riferimenti alle persone fisiche, ma non li cancella, perché vengono collocate in una apposita banca dati cifrata e protetta da password.
L'ANONIMIZZAZIONE consente all'organizzazione di trattenere nelle proprie banche dati solo le informazioni che non consentono di rintracciare le persone fisiche.

La CRITTOGRAFIA è un sistema che, tramite l'utilizzo di un algoritmo matematico, agisce su una

sequenza di caratteri, trasformandola. Tale trasformazione si basa sul valore di una chiave segreta, ovvero il parametro dell'algoritmo di cifratura/decifratura. Proprio la segretezza di questa chiave rappresenta il sigillo di sicurezza di ogni sistema crittografico.

La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

Significa che lungo tutto il ciclo di vita del dato personale (dalla sua raccolta alla sua distruzione), l'organizzazione deve assicurare:

a. la segretezza del dato, evitando l'accesso a tutti i soggetti non autorizzati;
b. la completezza dei contenuti e l'interezza sul piano della documentale;
c. la disponibilità e utilizzabilità da parte delle persone autorizzate;
d. la capacità degli strumenti di trattamento dei dati personali di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire nel tempo la disponibilità dei dati stessi.

La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Significa che l'organizzazione deve avere un piano di emergenza che le consenta gestire violazioni o minacce, assicurando la continuità delle operazioni di trattamento e disponibilità agli operatori.

Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Significa che l'organizzazione è tenuta a misurare periodicamente la capacità delle misure di sicurezza stabilite di assicurare su base continua il dovuto livello di protezione dei dati personali.

5. ANALISI DEI RISCHI

Per "rischio" si intende lo scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità e che hanno effetti sui *diritti e sulle libertà delle persone fisiche*. Il livello di esposizione al rischio di un'organizzazione è dato da almeno due variabili:

- la **probabilità di accadimento della minaccia rilevata** (la probabilità è legata anche all'esistenza o meno di strumenti di controllo/regole atti a prevenire il verificarsi della minaccia rilevata)
- il **danno,** inteso come danno materiale o immateriale all'interessato, derivante dal verificarsi dell'evento considerato a rischio.

A ciascuna di queste variabili può essere dato un peso, per esempio da 1 a 4: il coefficiente 1 indica improbabilità di accadimento dell'evento o danno trascurabile; il coefficiente 2 indica bassa probabilità o basso livello di danno; 3 media probabilità o livello medio di danno; 4 alta probabilità o livello significativo di danno.

La moltiplicazione di queste variabili e relativi coefficienti determina diversi livelli di rischio a cui è esposto l'interessato al trattamento.

L' Azienda intende procedere all'analisi dei rischi osservando il seguente schema di valutazione:

- se il risultato va da 1 a 3, il rischio è BASSO, pertanto è solo da monitorare;
- se il risultato va da 4 a 8, il rischio è MEDIO ovvero richiede un intervento di miglioramento entro un anno;
- se il risultato va da 9 a 16, il rischio è ALTO E SIGNIFICATIVO, e richiede un intervento urgente.

Probabilità	Alta	4	4	8	12	16
	Media	3	3	6	9	12
	Bassa	2	2	4	6	8
	Improbabile	1	1	2	3	4
			1	2	3	4
			Trascurabile	Basso	Medio	Significativo
			Danno			

Significativo -> Intervento urgente

Medio -> Pianificare intervento entro l'anno

Minimo -> Da monitorare

Il Regolamento stabilisce che, nel valutare l'adeguato livello di sicurezza, si deve tenere in special modo conto dei rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato.

L' Azienda intende procedere periodicamente all'analisi dei propri rischi, indagando i seguenti scenari:

1. RISCHIO DI DISTRUZIONE E PERDITA DI DATI
2. RISCHIO DI ACCESSO NON AUTORIZZATO
3. RISCHIO DI TRATTAMENTO NON CONSENTITO
4. RISCHIO DI TRATTAMENTO NON CONFORME ALLE FINALITA'
5. RISCHIO DI DIVERGENZA E NON CORRETTEZZA DEI DATI REGISTRATI.

Il processo logico che guida l'analisi dei rischi passa attraverso la verifica dei seguenti punti:

- *Quali eventi possono portare alla distruzione e perdita dei dati? Quali conseguenze?*
- *Quali misure di mitigazione del rischio sono gia' state implementate?*
- *Quale rischio residuo?*
- *Quali misure di miglioramento?*

Di seguito vengono approfondite le singole aree di rischio analizzate e vengono riportati a titolo di esempio alcuni eventi che possono avere impatto sulla libertà e dignità dell'interessato.

5.1 Rischio di distruzione e perdita di dati

Il Titolare del trattamento deve assicurare la conservazione, l'integrità e la disponibilità dei dati personali trattati, adottando idonee procedure aziendali in grado di prevenire i rischi – intenzionali od accidentali – di distruzione o di perdita dei dati.

Due sono le tipologie di eventi che cagionano la distruzione o perdita di dati:

- Eventi naturali;
- Eventi conseguenti al comportamento umano (dolo, incuria, colpa, …).

Fra gli **eventi accidentali** che possono cagionare la cancellazione o perdita dei dati personali da considerare ci sono:

- eventi distruttivi, naturali o artificiali (quali ad esempio movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, …)
- guasto ai sistemi complementari (quali ad esempio problemi all'impianto elettrico o di climatizzazione)
- malfunzionamento, indisponibilità o degrado degli strumenti elettronici (quali ad esempio casi di danneggiamento di hard disk o processori)
- carenza di consapevolezza, disattenzione o incuria (quali lo smarrimento di documenti).

Fra gli **eventi intenzionali** determinati dall'uomo:

- comportamenti sleali o fraudolenti (quali ad esempio distruzione volontaria di documenti da parte del personale dipendente o collaboratori)
- azione di virus informatici o di programmi suscettibili di recare danni (quali ad esempio l'installazione di virus in grado di alterare o cancellare i dati personali presenti in un data base)
- sottrazione di strumenti contenenti dati o documentazione cartacea (quali ad esempio furto di supporti removibili contenenti dati sensibili).

5.2 Rischio di accesso non autorizzato

Il Titolare del trattamento deve predisporre delle misure di sicurezza che garantiscano l'accesso agli archivi (cartacei e informatici) contenenti dati personali esclusivamente a persone da lui preventivamente autorizzate.

Fra gli **eventi** che possono determinare l'accesso non autorizzato ai dati personali si citano:

- sottrazione delle credenziali di autenticazione, ovvero di login e password
- carenza di consapevolezza, di disattenzione o incuria nella gestione degli accessi (quale ad esempio il lasciare aperto un archivio riservato ad accesso selezionato)
- comportamenti sleali o fraudolenti da parte del personale (quali ad esempio il consegnare copia delle chiavi di uffici o archivi a personale esterno)

- errori materiali ed umani nella gestione della sicurezza fisica (quali ad esempio non aver attivato il sistema dall'allarme prima della chiusura degli uffici)
- tecniche di sabotaggio (quali ad esempio l'installazione di software malevolo al fine di accedere al sistema informatico)
- ingressi non autorizzati a locali o reparti ad accesso ristretto (quali ad esempio l'elusione del sistema di gestione degli accessi aziendali).

5.3 Rischio di trattamento non consentito

Il Titolare del trattamento dovrà procedere ad instaurare delle misure volte a garantire la c.d. "CONFIDENZIALITÀ DEI DATI" ovvero studiate appositamente per prevenire il rischio di aggiunte, soppressioni o modifiche dei dati non autorizzate.

Fra gli **eventi** che possono determinare trattamenti non consentiti dei dati personali bisogna tenere conto di:

- disattenzione o incuria nel trattamento (come ad esempio nel caso di dimenticanza di cancellazione di tutti i file contenenti dati personali oggetto della richiesta di un interessato)
- errori materiali e umani nel trattamento (invio di una mail ad un indirizzo di destinatario errato)
- intercettazione di informazioni in rete, accessi non autorizzati al sistema informatico o spamming (come ad esempio nel caso di trattamento illecito di dati personali da parte di hackers)
- sottrazione di strumenti contenenti dati (come ad esempio nel caso di trattamento illecito di dati personali in seguito a furto di una copia di backup)
- manipolazione delle informazioni acquisite
- diffusione di dati sensibili.

5.4 Rischio di trattamento non conforme alle finalità

Il Titolare deve garantire che il trattamento dei dati raccolti sia sempre effettuato secondo le finalità dichiarate e comunicate all'interessato nell'informativa e sia limitato solamente ai dati per i quali il Titolare abbia ricevuto libero ed espresso consenso al trattamento.

Fra gli **eventi** che possono determinare tale rischio si citano:

- operazioni non autorizzate dall'interessato
- operazioni non pertinenti rispetto alle finalità del trattamento concordate.

5.5 Rischio di divergenza e non correttezza dei dati registrati

Il Titolare deve garantire la correttezza e completezza dei dati registrati.

Fra gli **eventi** che possono cagionare errori nella compilazione o registrazione del dato si cita:

- disattenzione o incuria nel trattamento (ad esempio: errori di compilazione di fatture o nel gestionale)
- volontà di alterare i contenuti della documentazione compilata per cagionare un danno.

6. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

A fronte di un elevato rischio per la tutela e libertà dell'interessato, l'Azienda è tenuta a svolgere la valutazione d'impatto del processo di trattamento critico.

La valutazione d'impatto consiste in un **processo** volto a:

- descrivere in maniera sistematica i trattamenti previsti e le relative finalità
- valutarne la necessità e la proporzionalità in relazione alle finalità
- gestire i rischi ad alto impatto sui diritti e le libertà degli interessati
- determinare le misure più idonee per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali
- dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

La valutazione di impatto fin dall'inizio si è ritenuta **obbligatoria** in tre casi:

- quando si ha una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche
- nel momento in cui si trattano, su larga scala, categorie particolari di dati personali, o dati relativi a condanne penali e reati
- nei casi in cui si ha una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'Autorità di controllo, nelle "**Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati"**, ha indicato nove criteri di cui tenere conto per verificare se è necessario o meno effettuare una valutazione d'impatto su un processo.
Se il processo soddisfa almeno due criteri fra quelli di seguito indicati, è necessario procedere alla valutazione d'impatto.

1. Valutazione personale basata sulla profilazione personale.
2. Decision making automatizzato con effetti legali sulle persone.
3. Monitoraggio (video sorveglianza) su vasta scala.
4. Dati sensibili o di natura altamente personale (ad esempio, opinioni politiche, "fedina" penale, dati sanitari personali, dati finanziari, documenti personali, email, codici di login personale).

5. Trattamento dati su ampia scala (ad esempio, durata del trattamento, area geografica, volume dei dati trattati in relazione alla popolazione).
6. Il matching e la combinazione di dataset diversi (ad esempio, provenienti da database diversi e raccolti in origine per scopi diversi, la cui combinazione rischia di eccedere la portata del consenso originario).
7. Dati che riguardano categorie di soggetti deboli (bambini, anziani, malati, malati di mente, richiedenti asilo).
8. Utilizzo innovativo dei dati e nuove tecnologie in azienda di cui non si conoscono le conseguenze personali e sociali (ad esempio, impronte digitali, riconoscimento facciale, Internet of Things).
9. Quando il trattamento stesso impedisce ai soggetti titolari dei dati di esercitare un diritto o di usare un servizio o un contratto (ad esempio, nel caso in cui una banca controlli l'affidabilità di un cliente consultando un database che raccoglie le referenze di credito).

Il Provvedimento del Garante Italiano per la protezione dei dati personali n.467/11.10.2018 ha fornito ulteriori specifiche sui processi che richiedono la Valutazione d'Impatto:

- trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato
- trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto di avvalersi di un bene o di un servizio o di continuare ad essere parte di un contratto in essere
- trattamenti che prevedono un uso sistematico dei dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti dei servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati
- trattamenti su larga scala di dati aventi carattere estremamente personale (es.: vita familiare o privata o che incidono sull'esercizio di un diritto fondamentale o la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato)
- trattamenti effettuati nell'ambito del rapporto di lavoro anche mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti
- trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)
- trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es.: IoT, sistemi di intelligenza artificiale, utilizzo di assistenti vocali

on-line attraverso lo scanning vocale e testuale, monitoraggi effettuati da dispositivi wearable, etc.)

- trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
- trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento
- trattamenti di dati sensibili o relativi a condanne penali
- trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento
- trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Non è necessaria la valutazione d'impatto:

1. nel caso in cui il trattamento dei dati personali non comporta un rischio elevato;
2. se esiste già una valutazione d'impatto simile;
3. nel momento in cui il trattamento è stato autorizzato prima del Maggio 2018;
4. se il trattamento ha una base legale;
5. se il trattamento non è compreso nella lista dei trattamenti che prevedono la Valutazione d'impatto.

Il Garante individua nelle sue Linee guida i **contenuti minimi** per rendere una Valutazione d'impatto accettabile. Il documento si compone di quattro parti.

- La prima parte è dedicata alla DESCRIZIONE SISTEMATICA DEL TRATTAMENTO, cioè alla descrizione della natura, contesto e finalità del trattamento oggetto di analisi; in questa parte devono essere indicati gli interessati e i destinatari, il periodo di conservazione dei dati e la descrizione funzionale, e infine gli strumenti coinvolti nel trattamento.

- La seconda parte consiste nella VALUTAZIONE, NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO: in questa fase si specificano le misure che determinano la liceità del trattamento e che contribuiscono a proteggere i diritti degli interessati.

- La terza parte è dedicata alla GESTIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI. In questa parte del documento si individua l'origine, la natura, le particolarità e gravità dei rischi (es. accesso illegittimo, modifiche indesiderate, indisponibilità dei dati), dal punto di vista degli interessati e le misure previste per gestire i rischi.

- Infine, la quarta parte RICHIEDE LA RACCOLTA DEL PARERE DEI SOGGETTI INTERESSATI attraverso il contributo scritto sia del Responsabile della Protezione dei Dati personali, sia

degli interessati al trattamento o dei rappresentanti degli stessi.

7. CONSULTAZIONE PREVENTIVA

Il Titolare del trattamento, prima di procedere al trattamento, può consultare l'Autorità garante qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenta comunque un **rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio**.

Nella consultazione preventiva il Titolare del trattamento è tenuto a comunicare al Garante:

a) le rispettive responsabilità del Titolare del trattamento (dei Contitolari del trattamento) e dei Responsabili del trattamento;
b) le finalità e i mezzi del trattamento previsto;
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
d) i dati di contatto del Responsabile della protezione dei dati;
e) la Valutazione d'impatto sulla protezione dei dati e ogni altra informazione richiesta dal Garante.

8. ALTRE MISURE

Sulla base dell'assetto organizzativo vigente e dei processi di trattamento dei dati personali connessi, la UOS AFFARI LEGALI – Ufficio Privacy, supportata, dove necessario, dalla UOC Sistemi Informativi Aziendali e dalle figure degli amministratori di sistema assicura:

- l'aggiornamento ANNUALE dell'analisi dei rischi tenendo conto dei requisiti stabiliti da codesto regolamento;
- l'identificazione ANNUALE dei processi ad alto rischio che richiedono la valutazione d'impatto.

Le analisi dei rischi e le valutazioni d'impatto dovranno tenere conto dei pareri formulati da Responsabile della Protezione dei Dati Personali.