Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Incaricato federale della protezione dei dati e della trasparenza
IFPDT

Versione 1.1

Raccomandazioni tecniche dell'IFPDT per la verbalizzazione secondo l'articolo 4 OPDa

del 15 ottobre 2026

Versione	Data	Descrizione
1.0	11.09.2023	Prima versione finalizzata
1.1	15.10.2026	Integrazione delle modifiche del 1o dicembre 2025 dell'Ordinanza sulla protezione dei dati del 31 agosto 2022

Indice

1. Introduzione e scopo del documento 3
1.1. Art. 4 OPDa 3
1.2. Art 3 cpv 3 OPDa 4
2. Verbalizzazione 4
2.1. I tre elementi chiave della verbalizzazione 4
2.1.1. Rilevamento 5
2.1.2. Registrazione 5
2.1.3. Analisi 5
2.2. Piano 5
3. Raccomandazioni tecniche 6
3.1. Raccomandazioni tecniche generali per la verbalizzazione 6
3.2. Registrazione e volume di memorizzazione 7
3.3. Verbalizzazione nel caso di applicazioni esistenti 8
4. Domande concrete sull'attuazione / FAQ 11

1. Introduzione e scopo del documento

Con l'entrata in vigore della revisione dell'articolo 4 OPDa[1] il 1° dicembre 2025[2], nel caso di trattamento automatico dei dati personali il titolare privato del trattamento e il suo responsabile privato del trattamento devono verbalizzare almeno la registrazione, modificazione, comunicazione, cancellazione. distruzione dei dati e ora, al posto della «lettura dei dati», «l'accesso ai dati»[3].

le presenti raccomandazioni per la prima volta

Questa modifica della formulazione e le presenti raccomandazioni mirano a facilitare la comprensione delle operazioni di registrazione da effettuare e a fornire una panoramica di ciò che deve essere registrato nuovamente per l'adempimento dell'articolo 4 OPDa. L'attuazione concreta deve essere definita dai diversi titolari dei sistemi e non è quindi parte integrante delle presenti raccomandazioni. Oltre alle disposizioni della legge federale sulla protezione dei dati (LPD), sono applicabili altre direttive, ad esempio quelle riguardanti la sicurezza delle informazioni. L'obiettivo è ottenere una verbalizzazione dei dati possibilmente efficiente ed efficace, evitando doppioni.

1.1. Art. 4 OPDa

Il tenore dell'articolo 4 OPDa relativo alla verbalizzazione è il seguente:

> [1] Se dati personali degni di particolare protezione sono trattati automaticamente su grande scala o se si esegue una profilazione a rischio elevato e i provvedimenti preventivi possono non garantire la protezione dei dati, il titolare privato del trattamento e il suo responsabile privato del trattamento verbalizzano almeno la registrazione, modificazione, lettura, comunicazione, cancellazione e distruzione dei dati nonché l'accesso ai dati. In particolare, la verbalizzazione deve avere luogo quando non è possibile stabilire a posteriori se i dati sono stati trattati ai fini per i quali sono stati raccolti o comunicati.
>
> [2] Nel caso di trattamento automatizzato di dati personali degni di particolare protezione, di esecuzione di profilazioni e di trattamento automatizzato di dati che rientrano nel campo d'applicazione della direttiva (UE) 2016/680[3], l'organo federale titolare del trattamento e il suo responsabile del trattamento verbalizzano almeno la registrazione, modificazione, comunicazione, cancellazione e distruzione dei dati nonché l'accesso ai dati. Nel caso di altri trattamenti automatizzati di dati valutano dapprima il rischio per i diritti fondamentali delle persone interessate. Su tale base e tenuto conto dello stato della tecnica e delle spese di implementazione stabiliscono se e in quale misura verbalizzare le succitate operazioni. Per la valutazione del rischio, tengono conto in particolare del tipo di dati trattati nonché dello scopo, del tipo, della portata e delle circostanze del trattamento.
>
> [2bis] La verifica della verbalizzazione secondo il capoverso 2 ha luogo per scritto. Il risultato e il contenuto della verifica sono comunicati, su richiesta, all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).
>
> [3] Nel caso di dati personali accessibili in modo generalizzato, nei casi di cui ai capoversi 1 e 2 primo periodo sono verbalizzate almeno la registrazione, modificazione, cancellazione e distruzione dei dati.
>
> [4] I verbali riportano informazioni sull'identità della persona che ha effettuato il trattamento, sul tipo, la data e l'ora del trattamento nonché, all'occorrenza, sull'identità del destinatario dei dati.
>
> [5] I verbali sono conservati per almeno un anno separatamente dal sistema in cui sono trattati i

[1] Ordinanza del 31 agosto 2022 sulla protezione dei dati (OPDa; RS **235.11**) (admin.ch)

[2] Termini di transizione secondo l'art. 46 cpv. 1 OPDa

[3] La lettura è una forma specifica di accesso.

dati personali. Sono accessibili esclusivamente agli organi e alle persone incaricate di verificare l'applicazione delle disposizioni in materia di protezione dei dati o di salvaguardare o ripristinare la confidenzialità, l'integrità, la disponibilità e la tracciabilità dei dati e sono utilizzati soltanto a tale fine.

1.2. Art 3 cpv 3 OPDa

La verbalizzazione serve a garantire la tracciabilità del trattamento e, in particolare, degliaccessi[4] ai dati personali. Questi due elementi sono sanciti all'articolo 3 capoverso 3 OPDa che descrive ciò che la verbalizzazione deve garantire:

> [3] Per garantire la tracciabilità, il titolare del trattamento e il responsabile del trattamento adottano provvedimenti adeguati affinché:
>
> a. si possa verificare quali dati personali sono stati introdotti o modificati nel sistema di trattamento automatizzato dei dati, in quale momento e da chi (controllo dell'introduzione);
> b. si possa verificare a chi sono stati comunicati dati personali con l'ausilio di impianti di trasmissione (controllo di comunicazione);
> c. si possano individuare rapidamente le violazioni della sicurezza dei dati (individuazione) e adottare provvedimenti per ridurre o eliminare le conseguenze (eliminazione).

2. Verbalizzazione

Nell'ambito del diritto in materia di protezione dei dati, la verbalizzazione si riferisce alla registrazione sistematica di informazioni sul trattamento di dati personali. La verbalizzazione serve a garantire la trasparenza, l'osservanza del principio di responsabilizzazione e la sicurezza dei dati; in caso di violazioni o incidenti legati alla protezione dei dati, essa permette di risalire a chi ha avuto accesso a determinati dati personali in un dato momento, di individuare eventuali modificazioni o di individuare e chiarire eventuali violazioni della sicurezza dei dati.

La verbalizzazione, invece, non deve essere utilizzata per monitorare il comportamento degli utenti che trattano dati personali.

2.1. I tre elementi chiave della verbalizzazione

I tre elementi chiave della verbalizzazione sono il rilevamento, la registrazione e l'analisi dei dati verbalizzati.

Il titolare privato del trattamento e il suo responsabile privato del trattamento devono verbalizzare almeno la registrazione, modificazione, comunicazione, cancellazione e distruzione dei dati, nonché l'accesso agli stessi. In particolare, la verbalizzazione deve avere luogo quando, senza tale misura, non è possibile stabilire a posteriori se i dati sono stati trattati ai fini per i quali sono stati raccolti o comunicati.

Sostituzione del termine «lettura»: la verbalizzazione della «lettura» dei dati personali ha dato luogo a questioni e difficoltà di attuazione. Per chiarire meglio che in questo contesto si intende un accesso senza modificazione, il termine viene sostituito con «accesso». L'accesso costituisce un trattamento dei dati ai sensi dell'articolo 5, lettera d, della LPD.

In tale contesto va osservata la restrizione secondo l'articolo 4 capoverso 3 OPDa concernente i dati personali accessibili in modo generalizzato al pubblico. Per questi dati

[4] Controllo degli accessi ai sensi dell'art. 3, cpv. 1, lett. a OPDa.

devono essere verbalizzati almeno la registrazione, modificazione, cancellazione e distruzione.

2.1.1. Rilevamento

I dati verbalizzati devono essere rilevati al fine di garantire la registrazione di tutte le operazioni eseguite sui dati personali. Questo significa che occorre verbalizzare tutti gli accessi (eseguiti da persone o macchine) ai dati personali; i verbali devono riportare informazioni sull'identità della persona oppure della macchina che effettua l'accesso (istanza tecnica[5]) che ha effettuato il trattamento, sul tipo, la data e l'ora del trattamento nonché, all'occorrenza, sull'identità del destinatario dei dati.

Quando una macchina effettua un accesso, spesso viene registrato anche il riferimento a una persona responsabile o a un'unità organizzativa. In questo modo è possibile risalire in un secondo momento a quale sistema abbia effettuato l'accesso, con quale identità tecnica sia avvenuto l'accesso e chi sia responsabile di tale identità tecnica.

2.1.2. Registrazione

I dati verbalizzati devono essere registrati in modo sicuro e protetto. Devono essere registrati separatamente dai sistemi di trattamento dei dati al fine di garantire che rimangano disponibili qualora il sistema primario dovesse essere compromesso (ad es. a causa di attacchi ransomware). Essi devono essere accessibili esclusivamente alle persone autorizzate, incaricate di verificare l'applicazione delle disposizioni in materia di protezione dei dati o di salvaguardare o ripristinare la confidenzialità, l'integrità, la disponibilità e la tracciabilità dei dati.

2.1.3. Analisi

All'occorrenza, i dati verbalizzati devono poter essere analizzati al fine di rilevare possibili violazioni della protezione e della sicurezza dei dati. Essi supportano titolari nell'osservanza dei principi di esattezza, proporzionalità e sicurezza dei dati (art. 4 LPD) e consentono di rendere conto a terzi, come autorità di vigilanza o revisori. Vengono in particolare utilizzati per verificare se, in un dato momento, siano stati compromessi riservatezza, integrità o disponibilità dei dati (ad esempio in seguito a un incidente di sicurezza). Per eseguire una simile analisi sono necessari strumenti performanti in grado di elaborare grandi quantità di dati verbalizzati e identificare schemi o anomalie che indicano possibili violazioni. Per verificare in casi specifici la legittimità dell'accesso ai dati personali, nella maggior parte dei casi sono sufficienti strumenti di analisi più semplici. Questi strumenti di analisi devono essere accessibili esclusivamente agli organi e alle persone incaricate di verificare l'applicazione delle disposizioni in materia di protezione dei dati o di salvaguardare o ripristinare la confidenzialità, l'integrità, la disponibilità e la tracciabilità dei dati e devono essere utilizzati soltanto a tale fine (art. 4 cpv. 5 OPDa).

2.2. Piano

Occorre elaborare un piano per la verbalizzazione che contenga una descrizione esaustiva e sistematica della politica e delle procedure in materia di verbalizzazione. Devono essere considerati in particolare i seguenti punti:

a) obiettivi della verbalizzazione: definire chiari obiettivi da raggiungere mediante la verbalizzazione, ad esempio il monitoraggio del trattamento dei dati personali, il monitoraggio della sicurezza e l'eliminazione degli errori;

b) direttive in materia di verbalizzazione: definire chiare direttive in materia di verbalizzazione. Deve stabilire, tra le altre cose, gli eventi da verbalizzare, i dati da

[5] ad es. sistema, applicazione, account di servizio, …

rilevare, la durata di registrazione prevista e quali persone sono autorizzate ad accedere a determinati dati verbalizzati;

c) strumenti per la verbalizzazione: descrivere gli strumenti utilizzati per la verbalizzazione, ad esempio gli agenti per la generazione dei verbali, gli strumenti di gestione dei log («log-management-tool»), il framework per il rilevamento degli eventi («event-logging-framework») o il software SIEM («security information and event management»);

d) piano di allarme: descrivere quali eventi possono generare allarmi, come reagire agli allarmi, quali persone avvisare in simili casi e quali misure adottare in caso di problemi;

e) responsabilità e ruoli: definire chiaramente le responsabilità e i ruoli per la gestione della verbalizzazione; deve indicare, ad esempio, le persone responsabili di monitorare la verbalizzazione, le persone incaricate di attribuire i diritti per il monitoraggio e le persone responsabili di aggiornare le direttive in materia di verbalizzazione. Il piano deve inoltre definire le persone responsabili dell'analisi e del reporting;

f) formazione: descrivere le formazioni che i collaboratori coinvolti nell'attività di verbalizzazione devono seguire affinché acquisiscano le conoscenze e competenze necessarie per lavorare in modo efficace e sicuro;

g) verifica: prevedere verifiche regolari della politica e delle procedure in materia di verbalizzazione al fine di garantire la loro efficacia e la loro conformità ai requisiti attuali.

È fondamentale redigere un piano globale che serva da base per verificare l'adeguatezza e la proporzionalità della politica in materia di verbalizzazione come pure la liceità dell'accesso ai dati verbalizzati.

3. Raccomandazioni tecniche

3.1. Raccomandazioni tecniche generali per la verbalizzazione

Esistono numerose raccomandazioni tecniche relative alla verbalizzazione in ambito di sicurezza o protezione dei dati. Di seguito sono riportati gli aspetti più importanti:

a) utilizzo di protocolli standard: i protocolli standard come Syslog o Common Event Format (CEF) contribuiscono a garantire una verbalizzazione uniforme degli eventi.

b) Lettura e interpretazione dei verbali: i verbali non vanno solo archiviati, ma anche letti e interpretati («parsing» e «indexing»). Questi due aspetti costituiscono la base per assicurare il monitoraggio e l'individuazione di anomalie nonché la trasmissione dell'allarme in caso di necessità. Durante la lettura (ingestione dei dati) tutti gli elementi informativi devono essere estrapolati mediante l'estrazione di modelli («pattern») e, laddove opportuno, completati con informazioni provenienti da verbali esistenti (correlazione). In questo processo, i campi d'informazione non utilizzati devono essere omessi, anche per risparmiare spazio di memoria.

c) Verifiche regolari dei dati verbalizzati: i dati verbalizzati devono essere verificati regolarmente per garantire che siano completi, conformi alle direttive in materia di sicurezza e che non siano stati manipolati.

d) Meccanismi per individuare anomalie: devono essere implementati meccanismi specifici che consentano di individuare anomalie nei dati verbalizzati (ad es. accesso da geolocalizzazione inconsueta) per rilevare attività sospette. A tal fine è necessario

innanzitutto definire il «comportamento normale» per poi poter determinare eventuali discrepanze.

e) Adozione di misure di sicurezza per i dati verbalizzati: è importante implementare opportuni controlli dell'accesso ai dati verbalizzati per garantire che questi siano protetti da accessi non autorizzati.

f) Marca temporale: i dati verbalizzati devono imperativamente essere corredati di marca temporale in modo che nel sistema venga rilevata l'ora esatta di un evento. La registrazione precisa dell'ora è fondamentale per comprendere le relazioni temporali tra i diversi eventi del sistema.

g) Sincronizzazione dell'ora: per assicurare che l'ora registrata dalla marca temporale sia esatta, è essenziale che tutti i sistemi della rete siano sincronizzati in modo attendibile e preciso. La sincronizzazione degli orologi di tutti i sistemi tramite un server NTP comune garantisce l'accuratezza e la coerenza dei dati.

h) «Data Enrichment»: i processi di «Data Enrichment» arricchiscono i dati verbalizzati con informazioni aggiuntive per consentire una migliore comprensione degli eventi. «Data Enrichment» permette di completare, ad esempio, i dati relativi a geoinformazioni, al contesto utente o alla configurazione di sistema e, quindi, di analizzare meglio i dati verbalizzati e individuare più rapidamente potenziali minacce alla sicurezza. Nel corso di tale processo è importante che vengano aggiunte solo le informazioni opportune e necessarie per il raggiungimento concreto degli obiettivi (nel caso concreto l'obiettivo è la verbalizzazione). L'arricchimento di dati mediante il collegamento con altri dati o la creazione di profili richiede, se è stato designato, il coinvolgimento del consulente per la protezione dei dati. Se il responsabile del trattamento è incaricato di procedere a un arricchimento dei dati, occorre anche assicurarsi che tra il committente e il responsabile del trattamento sia stato concluso un contratto giuridicamente valido che soddisfi i requisiti della LPD.

i) Trasmissione dell'allarme: le applicazioni utilizzate per analizzare i verbali devono essere in grado di informare immediatamente i responsabili in caso di anomalie o di eventi noti rilevanti per la sicurezza.

Attuando le presenti raccomandazioni tecniche, i titolari privati del trattamento possono ottenere una verbalizzazione completa che consente di monitorare e analizzare efficacemente gli eventi rilevanti per la sicurezza e di reagire tempestivamente.

3.2. Registrazione e volume di memorizzazione

Una delle difficoltà riscontrate nella verbalizzazione dei dati riguarda il volume di memorizzazione. Gli strumenti di analisi devono poter accedere direttamente ai dati verbalizzati solo per il tempo strettamente necessario per individuare eventuali violazioni della protezione dei dati e/o incidenti legati alla sicurezza e reagire tempestivamente. Quest'arco temporale può variare a seconda del tipo e della dimensione dell'organizzazione, ma solitamente si tratta di un intervallo compreso tra alcuni giorni e diverse settimane. Durante questo periodo i dati possono essere utilizzati attivamente per riconoscere attività sospette e adottare le misure necessarie.

Dal momento in cui non sono più strettamente necessari per effettuare analisi, ma ad es. solo per verificare l'applicazione delle disposizioni in materia di protezione dei dati, i dati verbalizzati possono essere spostati in un sistema di memorizzazione a lungo termine. Ciò consente di copiare e comprimere i dati in modo che il nuovo spazio di memorizzazione possa essere sfruttato più efficacemente. Va comunque osservato che non è ammesso

conservare i dati per una durata superiore a quella prevista dalla pertinente base giuridica, come ad esempio il Codice delle obbligazioni[6]. Al riguardo si raccomanda quanto segue:

a) utilizzo di supporti di memorizzazione adeguati: per la memorizzazione sul lungo termine di dati verbalizzati vanno utilizzati supporti di memorizzazione adeguati e affidabili con un lungo ciclo di vita;

b) durata di conservazione: è importante definire chiaramente la durata di conservazione dei dati verbalizzati per assicurarsi che questi non vengano conservati a lungo inutilmente. È sottointeso che vanno rispettate le disposizioni legali pertinenti. I dati verbalizzati in relazione al trattamento dei dati personali vanno conservati per almeno un anno;

c) calcolo del volume di memorizzazione: ai fini del calcolo del volume di memorizzazione necessario per i dati verbalizzati vanno considerati diversi fattori, ad esempio la quantità dei dati prodotti, il numero dei sistemi in rete e la durata di conservazione. È importante mettere a disposizione una capacità di memorizzazione sufficiente onde evitare eventuali interruzioni nel processo di verbalizzazione. Per la pianificazione del volume di memorizzazione e la stima dei relativi costi, ci si può basare sulla raccomandazione secondo cui normalmente i dati devono restare nel registro per una o due settimane per poi essere conservati per almeno un anno nel sistema di memorizzazione a lungo termine.

Riassumendo, si può affermare che la conservazione a lungo termine dei verbali è parte integrante della strategia in materia di salvaguardia dei dati. È inoltre importante che i dati vengano conservati separatamente dai sistemi di trattamento (v. art. 4 OPDa), al fine di garantirne l'integrità e la disponibilità. A condizione che la soluzione messa in atto per la conservazione sia affidabile e che l'integrità e la completezza dei dati vengano verificate periodicamente, di norma non è necessario creare una copia di sicurezza su un altro sistema. Tuttavia, occorrerà decidere di caso in caso se è necessario effettuare un backup.

3.3. Verbalizzazione nel caso di applicazioni esistenti

All'articolo 46 capoverso 1 OPDa vengono disciplinate le disposizioni transitorie per le applicazioni esistenti:

> [1] Per i trattamenti automatizzati di dati personali pianificati o iniziati prima dell'entrata in vigore della modifica del 29 ottobre 2025, la verifica della verbalizzazione di cui all'articolo 4 capoverso 2 deve aver luogo entro il 31 dicembre 2026. Se risulta necessaria, la verbalizzazione deve essere implementata entro il 31 dicembre 2029. Sono fatti salvi il trattamento automatizzato di dati personali degni di particolare protezione, l'esecuzione di profilazioni e i trattamenti automatizzati di dati che rientrano nel campo d'applicazione della direttiva (UE) 2016/680.

Nel caso di nuove applicazioni è relativamente semplice verbalizzare sin dall'inizio tutte le attività eseguite in relazione ai dati personali. Le applicazioni esistenti e più datate, invece, non sempre possono essere adattate alle nuove esigenze. In questi casi esistono comunque diversi approcci risolutivi.

L'attuazione della verbalizzazione dipende da diversi aspetti, quali il linguaggio di programmazione, l'ambiente di esecuzione e i metodi di sviluppo utilizzati per l'applicazione. Le presenti raccomandazioni hanno quindi carattere generico, ma possono agevolare la pianificazione per determinate applicazioni concrete.

[6] SR 220 Codice delle obbligazioni

Fase 1: conoscere i requisiti del processo di verbalizzazione per le applicazioni

Occorre valutare per quanto tempo i verbali debbano figurare nel registro ed essere conservati nel sistema di memorizzazione a lungo termine. La durata di conservazione (prescritta per legge) influisce sul calcolo del volume dei dati e della memorizzazione (ultima fase 5).

Fase 2: conoscere i processi di trattamento dei dati da verbalizzare

Non tutte le attività eseguite da un'applicazione riguardano il trattamento di dati personali da verbalizzare. Un elenco delle pertinenti attività può rivelarsi utile per concentrare eventuali modifiche ai processi su questo tipo di attività. L'obiettivo finale della verbalizzazione è rilevare le principali attività secondo l'OPDa indipendentemente dalla quantità.

Nel caso delle applicazioni che trattano dati personali senza che le pertinenti attività eseguite siano evidenti da subito (ad es. sistema di documentazione), è necessario verbalizzare tutte le attività.

Per rafforzare la sicurezza delle informazioni dell'applicazione, può essere auspicabile verbalizzare in aggiunta anche gli eventi critici per la sicurezza.

Fase 3: conoscere i flussi d'informazione che determinano un'attività di trattamento dei dati

Esistono diversi tipi di applicazioni.

- Nella maggior parte delle applicazioni, il trattamento di dati personali determina una comunicazione (ad es. flusso d'informazioni) tra l'interfaccia di presentazione dei contenuti (frontend) e la parte di amministrazione della logica dell'applicazione (backend). Questi flussi d'informazione passano spesso attraverso più reti e sistemi di sicurezza (cfr. a titolo di esempio la figura 1), in grado di visualizzare almeno una parte delle attività e che quindi possono essere utili ai fini della verbalizzazione in termini di sicurezza delle informazioni.

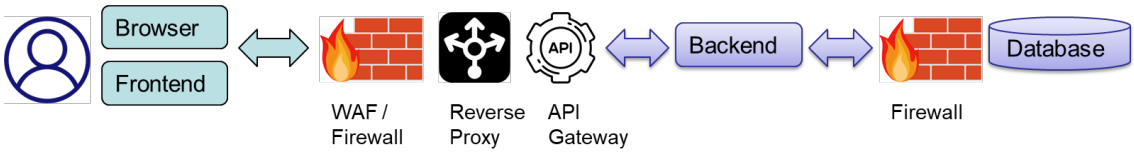

Figura 1 – Possibile flusso d'informazioni di un'applicazione

- Nel caso delle applicazioni in cui i dati sono trattati solo dall'utente senza che vi sia una comunicazione con il backend o le banche dati del server, il primo download sul sistema dell'utente deve essere verbalizzato come «accesso». In tal caso, generalmente le modificazioni dei dati potrebbero essere rilevate solo mediante un'estensione dell'applicazione stessa, il che sarebbe ragionevole solo in casi eccezionali.
- Un altro caso riguarda le applicazioni in cui i dati sono trattati autonomamente da un processo eseguito sul backend (come il collegamento automatizzato tra diversi dati personali e profili, l'estensione automatizzata di dati personali, ad es. aggiungendo i nomi corrispondenti alle ID utente). Anche per questo genere di applicazioni è spesso necessaria un'estensione.

Fase 4: decidere dove può e deve essere integrato il processo di verbalizzazione

Una volta che si conoscono le attività da verbalizzare e i flussi d'informazioni generati, è possibile valutare il modo più semplice per potenziare i processi di verbalizzazione. L'NCSC raccomanda la procedura descritta di seguito.

1. Generalmente le applicazioni esistenti permettono di verbalizzare le attività eseguite. Tuttavia, la pertinente funzionalità è spesso disattivata per default e va quindi abilitata. Per prima cosa, occorrere dunque verificare se questo è il caso. Se la funzionalità esistente permette di verbalizzare tutte le attività e contiene informazioni sufficienti (vale a dire l'identità della persona che riceve o tratta i dati personali nonché l'attività di trattamento), questo è l'approccio risolutivo più semplice.
2. È possibile che i sistemi di rete siano in grado di visualizzare abbastanza informazioni sull'attività (ad es. l'user ID mediante l'indirizzo IP e l'attività di backend). Se questo è il caso, per adempiere ai requisiti sono sufficienti i verbali di Firewall o della *Web Application Firewall* (WAF).
3. I server web o gli HTTP reverse proxy sono spesso in grado di visualizzare richieste non criptate. Anche tali sistemi consentono di verbalizzare le attività eseguite e possono rilevare in modo selettivo le richieste di comunicazione per poi trasmetterle a un sistema di analisi dei verbali.
4. Le applicazioni più moderne ricorrono anche ai gateway API. Questi ricevono tutte le richieste trasmesse dall'utente al backend o quelle intercorse tra i backend (nel caso del trattamento automatizzato) e poi le inoltrano al backend di destinazione corretto. Questi ultimi sono in grado di visualizzare il contenuto delle richieste. È possibile potenziare tale processo di verbalizzazione senza dover modificare l'applicazione stessa.
5. L'accesso ai dati personali o la loro modificaavviene perlopiù tramite sistemi di banche dati, i quali consentono quasi sempre di verbalizzare le relative richieste.
6. Se non è possibile attuare alcune delle raccomandazioni precedenti, occorre effettuare un'estensione dell'applicazione. Per non modificare l'applicazione stessa, talvolta è possibile creare uno «script wrapper». Si tratta di una nuova applicazione che riceve tutte le richieste per poi verbalizzarle e inoltrarle all'applicazione vera e propria, senza apportare alcuna modifica.

Fase 5: calcolare il volume di memorizzazione dei sistemi di analisi

Sulla base delle decisioni prese nelle fasi precedenti, si può procedere al calcolo del volume di memorizzazione (cfr. n. 3.3) e disciplinare la lettura e il monitoraggio dei verbali di concerto con il fornitore di prestazioni del sistema di destinazione.

4. Domande concrete sull'attuazione / FAQ

Di seguito sono elencate alcune domande pratiche che sono state sottoposte all'attenzione dell'NCSC. L'elenco delle domande verrà aggiornato all'occorrenza.

1) *Vanno attuate tutte le raccomandazioni formulate nel presente documento?*

Le raccomandazioni formulate nel presente documento sono di carattere generale. Al fine di garantire la cibersicurezza dei sistemi come pure una certa tracciabilità in funzione degli incidenti, la verbalizzazione è necessaria.
L'articolo 4 OPDa non prescrive se utilizzare o meno uno strumento di analisi né di che strumento debba trattarsi. Si parte dal presupposto che molti sistemi di trattamento dei dati pronti all'uso («out of the box») siano in grado di effettuare la verbalizzazione aggiuntiva richiesta.
L'OPDa obbliga solo a «spostare» i dati verbalizzati. A differenza di quanto previsto dal diritto in materia di cibersicurezza, il diritto sulla protezione dei dati non prescrive né la conservazione nello spazio di memorizzazione online né l'analisi dei dati verbalizzati.

2) *Cosa significa «accessibili in modo generalizzato»? Com'è possibile determinare con certezza il significato di tale espressione?*

L'accesso è possibile anche senza autenticazione, ad esempio su un server web.
Per «accessibili in modo generalizzato» s'intendono informazioni accessibili a un ampio pubblico, ad esempio la ricerca di un indirizzo tramite un sito Internet. Secondo la disposizione derogatoria di cui all'articolo 4 capoverso 3 OPDa, nel caso di questi dati personali vanno verbalizzate almeno la registrazione, la modificazione, la cancellazione e la distruzione. L'obiettivo di tale disposizione è permettere che ogni altro tipo di accesso e la comunicazione di tali dati personali non debbano essere verbalizzate.

3) *Quale livello di affidabilità («level of assurance», LoA) è ammesso per determinare l'identità (secondo l'art. 4 cpv. 4 OPDa) ai fini della verbalizzazione (Google-ID, Facebook o autenticazione a due fattori)?*

La verbalizzazione si riferisce all'/alle identità delle persone coinvolte nel trattamento dei dati ed è in tal senso indipendente dal LoA.

4) *Cosa accade se gli attuali sistemi non sono o non saranno in grado di adempiere tali requisiti?*

Praticamente qualsiasi sistema conosciuto può effettuare in qualche modo la verbalizzazione. In caso contrario, vi sono applicazioni terze in grado di svolgere tale processo. Se nel singolo caso non dovessero essere disponibili neanche tali applicazioni, occorrerebbe mettere a punto una soluzione adeguata o tenere conto delle raccomandazioni formulate al numero 3.3, al fine di rispettare le disposizioni pertinenti.

5) *Un backup dei dati verbalizzati può essere considerato una forma di registrazione che consente di conservare i dati separatamente dal sistema come previsto dall'articolo 4 capoverso 5 OPDa?*

Un backup adempirebbe il requisito previsto dall'articolo 2 capoverso 5 OPDa secondo cui i dati verbalizzati devono essere conservati separatamente dal sistema. Oltre ad aumentare la sicurezza contro eventuali attacchi, la conservazione separata dei verbali mira soprattutto a evitare che i dati vengano criptati nel caso di un incidente ransomware.

6) *Occorre verbalizzare anche l'esecuzione di script automatici?*

Se possono registrare, modificare, leggere, comunicare, cancellare, distruggere dati personali o accerderci, questi script vanno verbalizzati. L'obiettivo della verbalizzazione è garantire la tracciabilità delle operazioni di trattamento dei dati eseguite, ad esempio registrando l'inizio e la fine dell'attività di scripting, la versione dello script e l'identità della persona che ha effettuato il trattamento.

7) *Come gestire i sistemi NAS, SAN e gli altri sistemi di archiviazione non strutturati? Esempio: aprire un documento Word dalla directory O:\Divisione_A\Dati\Registro\xy.docx.*

L'articolo 4 capoverso 1 OPDa va messo in correlazione con l'articolo 3 capoverso 3 lettera a OPDa e va inteso nel senso che l'obbligo di verbalizzazione si applica solo ai dati personali elaborati nei sistemi di trattamento automatizzato dei dati. Nello scenario descritto nella domanda, gli accessi non devono quindi essere verbalizzati.

8) *Tutti i log vanno registrati nello stesso posto?*

Non necessariamente; si tratta inoltre di un approccio non realistico. Ai fini della verbalizzazione, l'importante è che i log siano presenti e che possano essere raggruppati in modo opportuno. I log dei firewall, ad esempio, possono essere registrati in un altro posto rispetto ai log dell'active directory, purché le modifiche e gli accessi ai dati personali possano essere ricostruiti. Ai fini della sicurezza delle informazioni, è inoltre importante che i log siano stati raggruppati in modo tale da poter riconoscere eventuali anomalie.

9) *Possono essere impiegate soluzioni esterne per la gestione dei log (soluzioni «log-management-as-a-service»)?*

A tal proposito occorre rivolgersi, laddove possibile, al servizio giuridico o al consulente per la protezione dei dati dell'impresa, dato che i rischi nell'ambito del trattamento dei dati personali tendono ad aumentare piuttosto che a diminuire. Sconsigliamo tale approccio. Sarebbe un'eccezione se il trattamento di per sé venisse già effettuato da un Saas («software as a service»), supponendo di aver comunque già consultato le persone succitate.

10) *I metadati di ogni documento contengono anche dati personali (dei collaboratori coinvolti) che vengono registrati in particolare quando si crea o modifica un documento o quando si inseriscono commenti. Supponiamo che la verbalizzazione secondo l'articolo 4 OPDa non si riferisca a questi dati personali.*

Corretto. Lo scopo della verbalizzazione è proteggere i dati personali trattati (contenuti in un documento). Il fatto che a seguito del trattamento di tali dati personali ne vengano generati altri (perché la persona X ha creato, modificato ecc. il documento) non ne rende necessaria la verbalizzazione. I dati personali generati per garantire la tracciabilità del trattamento dei dati non sono oggetto della verbalizzazione.