Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

ALLEGATO 1

ESEMPIO DI DPIA RELATIVA ALL'INSTALLAZIONE DI UN SISTEMA DI VIDEOSORVEGLIANZA (MEDIANTE UTILIZZO DEL SOFTWARE MESSO A DISPOSIZIONE DAL CNIL)

-- NOVEMBRE 2022

STEP 1 – ANALISI DEL CONTESTO

Panoramica del trattamento

1.1. QUAL È IL TRATTAMENTO PRESO IN CONSIDERAZIONE?

Il trattamento ha ad oggetto i dati personali (immagini) raccolti mediante l'attivazione e il funzionamento di un impianto di videosorveglianza attivo presso la sede della Società/Ente. L'impianto di videosorveglianza è installato per il perseguimento delle seguenti finalità [indicare una o più finalità tra quelle indicate all'articolo 4 dello Statuto dei Lavoratori]:

- tutela del patrimonio aziendale
- sicurezza del lavoro
- esigenze organizzative e produttive

L'impianto è costituito da [descrivere le caratteristiche tecniche dell'impianto, con il numero di telecamere, la specificazione se interne o esterne, il numero dei monitor, il numero di DVR (digital video recorder) /NVR (network video recorder), la fascia oraria di funzionamento, i tempi di conservazione delle immagini registrate]. Indicare se sono presenti accordi sindacali o autorizzazioni da parte della Direzione Territoriale del Lavoro competente.

Criticità del trattamento: risiede nel fatto che dal funzionamento dell'impianto di videosorveglianza potrebbe derivare un controllo a distanza delle attività dei lavoratori, riconducibile all'articolo 35, paragrafo 3, lettera c), GDPR, nella fattispecie di "Monitoraggio sistematico, trattamenti utilizzati per osservare monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o sorveglianza sistematica di un'area accessibile al pubblico".

1.2. QUALI SONO LE RESPONSABILITÀ CONNESSE AL TRATTAMENTO?

- Titolare del Trattamento: [indicare la ragione sociale, la sede legale e il dato di contatto del Titolare del trattamento e suoi dati di contatto].
- Responsabile del Trattamento: [indicare nominativo e attività di trattamento svolte per conto del Titolare, come ad esempio l'affidamento di un servizio in outsourcing, come la vigilanza esterna].
- Data Protection Officer: Il Titolare si avvale di un Responsabile per la protezione dei dati personali (anche noto come Data Protection Officer "DPO") che vigila sulla conformità aziendale alla normativa a protezione dei dati personali. Il DPO può essere contattato tramite il seguente canale di comunicazione: [indicare, se nominato].
- Incaricati del trattamento: tutte le persone fisiche che hanno accesso alle immagini, anche se non autorizzate a compiere alcuna operazione sulle stesse, sono designate incaricati del trattamento ("Incaricati").

La designazione degli Incaricati è effettuata per iscritto dal Titolare e individua puntualmente l'ambito del trattamento loro consentito. Ad esempio, nel caso specifico, accesso ai monitor e/o possibilità di

compiere operazioni tecniche sul Sistema CCTV (closed circuit television), quali ad esempio, a seconda dei casi, attività di manutenzione, attività di acquisizione delle immagini.

1.3. CI SONO STANDARD APPLICABILI AL TRATTAMENTO?

Al trattamento in materia di videosorveglianza si applicano le seguenti normative e provvedimenti:

- Art. 4 L. 300/1970 (c.d. Statuto dei Lavoratori), così come modificato dall'art. 23 del D.lgs. 151/2015 (c.d. Jobs Act);
- Regolamento UE n. 2016/679 (GDPR);
- D.Lgs. n. 196/2003 (c.d. Codice Privacy) così come novellato dal D.Lgs. 101/2018;
- EDPB, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video (adottate il 29 gennaio 2020);
- Provvedimento generale in materia di videosorveglianza dell'8 aprile 2010.

Dati, processo e risorse di supporto

1.4. QUALI SONO I DATI TRATTATI?

Le immagini di videosorveglianza consentono l'identificazione della persona fisica (dipendente/visitatore/collaboratore esterno/fornitore) che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, oltre che più elementi caratteristici della sua identità fisica e fisiologica.

1.5. QUAL È IL CICLO DI VITA DEL TRATTAMENTO DEI DATI (DESCRIZIONE FUNZIONALE)?

Il Titolare del trattamento [indicare nominativo] raccoglie i dati personali mediante il funzionamento dell'impianto di videosorveglianza attivo presso la/le sede/sedi della Società. Le immagini, oltre che essere viste in tempo reale vengono registrate mediante il Sistema CCTV, il quale trasmette le immagini acquisite su monitor dedicati e controllati dal personale incaricato della videosorveglianza.

L'accesso alle immagini registrate avviene solo nel caso si verifichino eventi criminosi o eventi che rendano necessario un intervento.

I dati personali non vengono diffusi e/o divulgati, ma vengono comunicati esclusivamente all'Autorità giudiziaria e/o di polizia per rispondere a particolari esigenze d'indagine.

Alla fine del periodo di conservazione [indicare tempo di conservazione stabilito in accordo sindacale o nel provvedimento di autorizzazione da parte della DTL territorialmente competente] le immagini vengono cancellate mediante sovrascrizione automatica.

1.6. QUALI SONO LE RISORSE DI SUPPORTO AI DATI?

Il Sistema CCTV comporta la raccolta e il trattamento dei dati personali raccolti tramite videosorveglianza, quindi su supporto elettronico. I supporti sono di seguito elencati [elencare strumenti informatici di supporto alle immagini, come DVR o NVR].

STEP 2 – PRINCIPI FONDAMENTALI

Proporzionalità e necessità

2.1. GLI SCOPI DEL TRATTAMENTO SONO SPECIFICI, ESPLICITI E LEGITTIMI?

Gli scopi sono specifici, espliciti e legittimi, in quanto i dati personali sono raccolti e trattati dalla Società esclusivamente per finalità di sicurezza, controllo degli accessi, tutela aziendale, incolumità fisica delle persone ai sensi della normativa sulla sicurezza nei luoghi di lavoro, tutela di proprietà e patrimonio aziendali [specificare quali di queste finalità sono effettivamente perseguite dal Titolare, possono essere una o tutte].

2.2. QUALI SONO LE BASI LEGALI CHE RENDONO LECITO IL TRATTAMENTO?

Base giuridica: il trattamento si fonda sulla base giuridica del legittimo interesse del Titolare del trattamento (articolo 6, paragrafo 1, lett. f), GDPR).

2.3. I DATI RACCOLTI SONO ADEGUATI, PERTINENTI E LIMITATI A QUANTO È NECESSARIO IN RELAZIONE ALLE FINALITÀ PER CUI SONO TRATTATI (MINIMIZZAZIONE DEI DATI)?

In applicazione del principio della pertinenza delle immagini raccolte, il Sistema CCTV non è installato, ad esempio, in quei luoghi dove i rischi connessi alle finalità di cui sopra sono del tutto assenti e, al contrario, è incentivata l'adozione di strumenti tecnologici conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi.

In particolare, le telecamere sono installate affinché l'angolatura e la panoramica delle riprese venga effettuata con modalità tali da limitare l'angolo di visuale all'area da proteggere [indicare le caratteristiche tecniche, le modalità di funzionamento e l'ubicazione delle telecamere che compongono il Sistema CCTV delle sedi aziendali].

2.4. I DATI SONO ESATTI E AGGIORNATI?

I dati sono raccolti in tempo reale e archiviati decorso il termine di conservazione previsto, quindi sono costantemente esatti e aggiornati.

2.5. QUAL È IL PERIODO DI CONSERVAZIONE DEI DATI?

La conservazione delle immagini registrate dal Sistema CCTV è limitata al tempo [indicare tempo di conservazione stabilito in accordo sindacale o nel provvedimento di autorizzazione da parte della DTL territorialmente competente].

Il Sistema CCTV è programmato in modo da prevedere l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Misure a tutela dei diritti degli interessati

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

2.6. COME SONO INFORMATI DEL TRATTAMENTO GLI INTERESSATI?

Gli interessati al trattamento sono informati tramite le seguenti modalità:

- informativa semplificata (cartelli) che vengono apposti in prossimità delle aree videosorvegliate;
- informativa estesa redatta ai sensi dell'articolo 13 GDPR, che viene fatta sottoscrivere ai dipendenti per presa visione.

2.7. OVE APPLICABILE: COME SI OTTIENE IL CONSENSO DEGLI INTERESSATI?

Per il trattamento in oggetto non è richiesto il consenso dell'interessato, in quando si fonda su un presupposto di liceità diverso (legittimo interesse del Titolare - articolo 6, paragrafo 1, lett. f), GDPR).

2.8. COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI ACCESSO E DI PORTABILITÀ DEI DATI?

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo a [indicare dato di contatto a cui gli interessati possono scrivere per esercitare i diritti riconosciutigli dal GDPR, come ad esempio un indirizzo mail privacy@].

Indicare la presenza di eventuali policy aziendali per la gestione delle richieste da parte degli interessati.

2.9. COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI RETTIFICA E DI CANCELLAZIONE (DIRITTO ALL'OBLIO)?

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo a [indicare dato di contatto a cui gli interessati possono scrivere per esercitare i diritti riconosciutigli dal GDPR, come ad esempio un indirizzo mail privacy@].

Indicare la presenza di eventuali policy aziendali per la gestione delle richieste da parte degli interessati.

2.10. COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI LIMITAZIONE E DI OPPOSIZIONE?

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo a [indicare dato di contatto a cui gli interessati possono scrivere per esercitare i diritti riconosciutigli dal GDPR, come ad esempio un indirizzo mail privacy@].

Indicare la presenza di eventuali policy aziendali per la gestione delle richieste da parte degli interessati.

2.11. GLI OBBLIGHI DEI RESPONSABILI DEL TRATTAMENTO SONO DEFINITI CON CHIAREZZA E DISCIPLINATI DA UN CONTRATTO?

[Indicare come sono stati nominati i Responsabili del trattamento a cui sono affidati servizi in outsourcing che comportano un trattamento di dati personali per conto del Titolare e cosa è previsto all'interno del contratto che disciplina le responsabilità tra le parti, con particolare riferimento alle istruzioni che il Titolare fornisce al Responsabile, sulla base di quanto disposto dall'articolo 28 GDPR].

2.12. IN CASO DI TRASFERIMENTO DI DATI AL DI FUORI DELL'UNIONE EUROPEA, I DATI GODONO DI UNA PROTEZIONE EQUIVALENTE?

[Indicare se il trattamento dei dati personali effettuato mediante il funzionamento dell'impianto di videosorveglianza comporta un trattamento di dati personali fuori dallo SEE (Spazio Economico Europeo), ad esempio un trasferimento delle immagini negli Stati Uniti d'America sulla base di specifici contratti infragruppo con una società controllante; descrivere quali delle condizioni di cui all'art. 44 e ss. del GDPR sono applicate al trasferimento verso Paesi Terzi, come decisioni di adeguatezza, clausole contrattuali standard].

STEP 3 – RISCHI

La valutazione dei rischi può essere operativamente effettuata utilizzando la metodologia proposta ENISA (si veda il § 6.3. del documento), oppure – per le realtà di medie e piccole dimensioni – applicando la metodologia presente nello stesso software meso a disposizione dal Garante francese (CNIL), di seguito illustrata.

Lo step 3 richiede:

individuazione delle misure di sicurezza esistenti o pianificate	misure tecniche (password, backup, crittografia, ecc.)
	misure organizzative (policy aziendali)
indicazione dei rischi	rischi in caso di accesso illegittimo ai dati
	rischi in caso di modifiche indesiderate dei dati
	rischi in caso di perdita dei dati
valutazione dei rischi	stima dell'impatto
	stima della probabilità

Con riferimento alle misure di sicurezza da indicare si rinvia al § 8 del documento.

Con riferimento a ciascun rischio GDPR vengono richieste le seguenti informazioni:

3.1. QUALI POTREBBERO ESSERE I PRINCIPALI IMPATTI SUGLI INTERESSATI SE IL RISCHIO SI DOVESSE CONCRETIZZARE?

Ansia/tensione, discriminazione, senso di violazione privacy, diffamazione, insicurezza, altro.

3.2. QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONCRETIZZARE IL RISCHIO?

Dipendente Infedele, fornitore infedele, attacco esterno, smarrimento password di accesso ai sistemi informatici, furto di credenziali, furto chiavi armadio, accesso alla sala CED da parte di personale non autorizzato, ecc.

3.3. QUALI SONO LE FONTI DI RISCHIO?

Fonti umane interne, fonti umane esterne, fonti non umane.

3.4. QUALI MISURE FRA QUELLE INDIVIDUATE CONTRIBUISCONO A MITIGARE IL RISCHIO?

Controllo degli accessi, integrità e disponibilità dei dati, cancellazione e diritto di accesso (a titolo esemplificativo: archiviazione, gestione del personale, sicurezza dei documenti cartacei, gestione dei

rischi, controllo degli accessi fisici, gestione postazioni, minimizzazione dei dati, tracciabilità, protezione contro fonti di rischio non umane).

Per maggiori dettagli si rimanda all'elenco delle misure tecniche e organizzative di cui Allegato 2.

Per ciascun rischio viene richiesto di esprimere il seguente giudizio:

Soggetti che partecipano alla valutazione d'impatto

Sicuramente la valutazione d'impatto dovrà essere condotta da un soggetto che conosce la normativa in materia di trattamento dei dati personali, compresi i provvedimenti e le linee guida emanati dal Garante della privacy. Occorre raccogliere documenti e pareri tecnici; nel caso in esempio la valutazione d'impatto di un sistema di videosorveglianza richiede, sicuramente, la partecipazione del soggetto che installa il sistema.

Dovrà poi essere coinvolto il DPO, ove nominato, al fine di ottenere un parere in merito alla DPIA.

Se del caso, il titolare del trattamento è tenuto a raccogliere le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o di pubblico interesse o la sicurezza dei trattamenti.