**VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI**

**ART. 35 REG UE 16/679**

**PROCEDURA DI VALUTAZIONE DEI RISCHI**

**LA PRESENTE VALUTAZIONE DI IMPATTO CONCERNE IL SEGUENTE TRATTAMENTO[[1]](#footnote-3):**

* Trattamenti effettuati nell’ambito del rapporto di lavoro 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 che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
* Trattamenti di categorie particolari di dati ai sensi dell’art. 9 oppure di dati relativi a condanne penali e a reati di cui all’art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
* 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*; tracciamenti di prossimità come ad es. il *wi-fi tracking*).
* 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 (es. *mobile payment*).
* 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 o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).
* Trattamenti che prevedono un utilizzo sistematico di 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 di servizi della società dell’informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
* Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
* 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.

La presente valutazione di impatto tiene in considerazione il seguente modello organizzativo:

pasted-image.tiff

**1) DESCRIZIONE DEL TRATTAMENTO[[2]](#footnote-4):**

Il trattamento oggetto di questa valutazione di impatto concerne la seguente attività:

| descrizione del trattamento oggetto della presente valutazione di impatto | QUALI SONO LE finalità perseguitE con il predetto trattamento? | si è considerata la necessità e la proporzionalità  del trattamento in base al fine perseguito? | quali sono i soggetti autorizzati al trattamento? | chi è il soggetto responsabile della supervisione del trattamento? | QUALI SONO I SOGGETTI INTERESSATI AL TRATTAMENTO? | **PERIODO DI CONSERVAZIONE DEI DATI TRATTATI** | **LA PRESENTE VALUTAZIONE HA COINVOLTO IL DPO?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |

**2) VALUTAZIONE DELLE POTENZIALI CONSEGUENZE DERIVANTI DALLA MANCATA ADOZIONE DI ADEGUATE MISURE DI SICUREZZA:**

Il trattamento oggetto di questa valutazione di impatto potrebbe essere soggetto ai seguenti rischi per i diritti e le libertà degli interessati sopra individuati:

| ELENCAZIONE DEI RISCHI POTENZIALMENTE INCOMBENTI SUL TRATTAMENTO SOPRA DESCRITTO | SI | TENORE DEL RISCHIO:  1 MOLTO BASSO  2 BASSO  3 MEDIO  4 ALTO  5 MOLTO ALTO | NO |
| --- | --- | --- | --- |
| lesione della dignità dell’interessato (ad es. pregiudizio alla reputazione) |  |  |  |
| rischio discriminazione dell’interessato |  |  |  |
| rischio furto o usurpazione dell’identità dell’interessato |  |  |  |
| lesione del diritto alla salute dell’interessato |  |  |  |
| danno economico per l’interessato |  |  |  |
| danno di immagine per il titolare |  |  |  |
| **VALUTAZIONE DEL COMPLESSIVO LIVELLO DI RISCHIO CONNESSO AL TRATTAMENTO SVOLTO** |  |  |  |

**3) INDIVIDUAZIONE DEI FATTORI DI RISCHIO E INDICAZIONE DELLE MISURE DI SICUREZZA:**

**3A: RISCHI CONNESSI AL COMPORTAMENTO DEI SOGGETTI AUTORIZZATI:**

| FATTORE DI RISCHIO | MISURE DI SICUREZZA | TENORE DEL RISCHIO:  1 MOLTO BASSO  2 BASSO  3 MEDIO  4 ALTO  5 MOLTO ALTO | POSSIBILI ELEMENTI CORRETTIVI A RIDUZIONE DEL RISCHIO | **TEMPISTICA DELL’INTERVENTO** | **RESPONSABILE DELL’AZIONE** |
| --- | --- | --- | --- | --- | --- |
| MANCATA OSSERVANZA DEL SISTEMA DI AUTENTICAZIONE PERSONALE |  |  |  |  |  |
| CONDIVISIONE/INCURIA NELLA GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE PERSONALE |  |  |  |  |  |
| DISATTENZIONE O INCURIA NELLA PROTEZIONE DEI DOCUMENTI ELETTRONICI O CARTACEI CONTENENTI DATI PERSONALI |  |  |  |  |  |
| COMPORTAMENTI SLEALI O FRAUDOLENTI |  |  |  |  |  |
| ERRORE MATERIALE |  |  |  |  |  |
| INOSSERVANZA DELLE ISTRUZIONI IMPARTITE DAL TITOLARE O DAL DPO (OVE PRESENTE) |  |  |  |  |  |
| INOSSERVANZA PROCEDURE E/O DELLE POLICY INTERNE |  |  |  |  |  |
| ACCESSO AGLI ARCHIVI DI CUI NON AUTORIZZATI |  |  |  |  |  |
| COMUNICAZIONE O DIFFUSIONE NON AUTORIZZATA |  |  |  |  |  |

**3B: RISCHI CONNESSI ALL’UTILIZZO DEI SISTEMI INFORMATICI IN USO**

| FATTORE DI RISCHIO | MISURE DI SICUREZZA | TENORE DEL RISCHIO:  1 MOLTO BASSO  2 BASSO  3 MEDIO  4 ALTO  5 MOLTO ALTO | POSSIBILI ELEMENTI CORRETTIVI A RIDUZIONE DEL RISCHIO | **TEMPISTICA DELL’INTERVENTO** | **RESPONSABILE DELL’AZIONE** |
| --- | --- | --- | --- | --- | --- |
| ESPOSIZIONE A VIRUS |  |  |  |  |  |
| PERDITA O DANNEGGIAMENTO DEI DATI PER OBSOLESCENZA DEGLI STRUMENTI ELETTRONICI |  |  |  |  |  |
| OBSOLESCENZA DEI SOFTWARE CON I QUALI HA LUOGO IL TRATTAMENTO |  |  |  |  |  |
| UTLIZZO SUPPORTI NON CIFRATI |  |  |  |  |  |
| SPAMMING O SABOTAGGI DA PARTE DI TERZI |  |  |  |  |  |
| ALLOCAZIONE DEI DATI IN CLOUD |  |  |  |  |  |
| UTLIZZO DI DISPOSITIVI REMOVIBILI |  |  |  |  |  |
| MALFUNZIONAMENTO E DEGRADO DEGLI STRUMENTI |  |  |  |  |  |
| ACCESSI ESTERNI NON AUTORIZZATI |  |  |  |  |  |
| INTERCETTAZIONE DEI DATI DALLA RETE |  |  |  |  |  |
| VULNERABILITA’ DELLE PERIFERICHE |  |  |  |  |  |
| FURTO STRUMENTI |  |  |  |  |  |
| PERDITA STRUMENTI (AD. ES. NOTEBOOK, TABLET, USB, ECC.) |  |  |  |  |  |

**3C: RISCHI CONNESSI AL CONTESTO DOVE HA LUOGO IL TRATTAMENTO (LOCALI, ARCHIVI, ECC.)**

| FATTORE DI RISCHIO | MISURE DI SICUREZZA | TENORE DEL RISCHIO:  1 MOLTO BASSO  2 BASSO  3 MEDIO  4 ALTO  5 MOLTO ALTO | POSSIBILI ELEMENTI CORRETTIVI A RIDUZIONE DEL RISCHIO | **TEMPISTICA DELL’INTERVENTO** | **RESPONSABILE DELL’AZIONE** |
| --- | --- | --- | --- | --- | --- |
| ACCESSO NON PRESIDIATO E POSSIBILITÀ’ CHE TERZI ACCEDANO AI DATI |  |  |  |  |  |
| RISCHIO CONDIVISIONE NON AUTORIZZATA PER LA PROMISCUITÀ’ DEI LOCALI |  |  |  |  |  |
| FURTO/PERDITA DEI DOCUMENTI CARTACEI |  |  |  |  |  |
| ALLAGAMENTO ARCHIVI |  |  |  |  |  |
| INCENDIO ARCHIVI |  |  |  |  |  |

**3D: RISCHI CONNESSI ALLA ATTIVITA’ DI VIDEOSORVEGLIANZA**

| FATTORE DI RISCHIO | MISURE DI SICUREZZA | TENORE DEL RISCHIO:  1 MOLTO BASSO  2 BASSO  3 MEDIO  4 ALTO  5 MOLTO ALTO | POSSIBILI ELEMENTI CORRETTIVI A RIDUZIONE DEL RISCHIO | **TEMPISTICA DELL’INTERVENTO** | **RESPONSABILE DELL’AZIONE** |
| --- | --- | --- | --- | --- | --- |
| PERDITA DELLE IMMAGINI |  |  |  |  |  |
| INTERFERENZE ILLECITE NELLA VITA PRIVATA |  |  |  |  |  |
| ACCESSO ALLE IMMAGINI DA PARTE DI TERZI |  |  |  |  |  |
| ILLECITA DIFFUSIONE DELLE IMMAGINI |  |  |  |  |  |
| ATTIVITA’ ANTISINDACALE E CONTROLLO ILLECITO PERSONALE DIPENDENTE |  |  |  |  |  |

**3E: RISCHI CONNESSI AL TRATTAMENTO INFORMATIZZATO DELLA DOCUMENTAZIONE SANITARIA (MEDIANTE FSE -DS)**

| FATTORE DI RISCHIO | MISURE DI SICUREZZA | TENORE DEL RISCHIO:  1 MOLTO BASSO  2 BASSO  3 MEDIO  4 ALTO  5 MOLTO ALTO | POSSIBILI ELEMENTI CORRETTIVI A RIDUZIONE DEL RISCHIO | **TEMPISTICA DELL’INTERVENTO** | **RESPONSABILE DELL’AZIONE** |
| --- | --- | --- | --- | --- | --- |
| PERDITA DELLE INFORMAZIONI |  |  |  |  |  |
| CONDIVISIONE CON TERZI NON AUTORIZZATI |  |  |  |  |  |
| ERRORE NELLA GESTIONE DELLA DOCUMENTAZIONE |  |  |  |  |  |
| MANCATO RISPETTO DELLE MISURE DI SICUREZZA PREVISTE DALLA NORMATIVA VIGENTE (ES. TRACCIABILITÀ’ E CONSERVAZIONE DEI LOG) |  |  |  |  |  |

1. per l’individuazione dei trattamenti oggetto di DPIA si fa riferimento ai criteri elaborati dal Garante per la protezione dei dati personali mediante il Provvedimento n. 467 del 11 ottobre 2018 e relativo allegato 1 [↑](#footnote-ref-3)
2. art. 35 comma 7 Reg UE 16/679 [↑](#footnote-ref-4)