ADOS SRL
CONSULENZE PER L'IMPRESA

Audit - Data protection - Outsourcing Services

Oggetto: **Adempimenti in materia di privacy: la valutazione di impatto sulla protezione dei dati (DPIA)**

Spett.le Cliente,

in qualità di *Data Protection Officer* della Vostra Struttura, Vi ricordiamo uno degli obblighi imposti dalla normativa in materia di protezione dei dati personali, al fine di procedere, in caso non abbiate ancora provveduto, al corretto adempimento dell'onere in oggetto: l'esecuzione di una valutazione di impatto sulla protezione dei dati personali.

Il Regolamento Generale sulla Protezione dei Dati Personali n.679/2016 (GDPR), infatti, impone, all'art. 35, che il Titolare del trattamento, allorché un trattamento di dati personali, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, effettui, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

In sostanza, occorre che venga effettuata una valutazione sull'impatto che un determinato tipo di trattamento potrebbe comportare per i diritti e le libertà dei soggetti interessati.

La valutazione di impatto (*Data Protection Impact Assessment*, di seguito anche, per brevità, DPIA) **deve essere svolta dal Titolare del trattamento**, che è a conoscenza di tutte le caratteristiche dei trattamenti che svolge.

Suggeriamo di redigere la valutazione con l'assistenza del responsabile del reparto IT, che potrà adeguatamente supportare il Titolare del trattamento sulle misure di sicurezza tecniche adottate, al fine di valutare i rischi connessi al trattamento in esame e progettare ulteriori misure di sicurezza al fine di mitigarli.

La DPIA può essere agevolmente effettuata mediante l'utilizzo dell'applicativo software fornito gratuitamente dall'Autorità di controllo francese (CNIL) e resa disponibile nella lingua italiana dal Garante per la Protezione dei Dati Personali. Tale applicazione guida il Titolare del trattamento nella effettuazione della valutazione, mediante la proposta di alcune domande a cui rispondere, che coadiuvano il Titolare del trattamento nella valutazione del grado di rischio connesso trattamento oggetto di DPIA.

È possibile scaricare l'applicazione, che è gratuita, al seguente *link* **https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil .** Una volta aperta la pagina, che apparirà in lingua francese, occorre scorrere fino al titolo "*Version portable*" o "*Version logiciel*" e selezionare il tipo di sistema operativo installato sul proprio computer. Una volta scaricato il *software*, lanciare l´installazione che sarà effettuata automaticamente nella versione in lingua italiana. Occorre sottolineare che il *software* è in continua evoluzione, con revisioni introdotte anche sulla base dell´esperienza raccolta e delle segnalazioni degli utenti. Pertanto, in caso necessitaste di effettuare DPIA a distanza di tempo, si consiglia di scaricare nuovamente il programma.

La valutazione dovrà contenere almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Di seguito, un **elenco dei trattamenti che devono obbligatoriamente essere oggetto di valutazione di impatto,** con particolare evidenza dei trattamenti che potrebbero essere svolti nella Struttura:

1) 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.
2) Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
3) 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.
4) Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
5) Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Qualora la struttura svolga uno o più dei suddetti trattamenti è obbligatorio procedere alla DPIA. Naturalmente deve essere redatta una DPIA per ciascun trattamento a rischio.

In ogni caso si allega alla presente l'elenco completo di tutti i trattamenti che a parere del Garante devono essere sottoposti a DPIA.

Al termine del procedimento di valutazione, il documento generato dovrà essere inviato al *Data Protection Officer*, il quale esprimerà un parere in merito alla valutazione di impatto.

Nel caso in cui la Vostra Struttura esegua uno (o più) dei trattamenti suddetti e non sia ancora stata eseguita una (o più) DPIA, occorre prontamente provvedere all'esecuzione della valutazione per tutti i trattamenti suddetti eventualmente da Voi svolti.

Suggeriamo comunque di ripetere la valutazione con l'utilizzo dell'applicativo indicato anche nel caso in cui il documento DPIA sia già stato adottato.

Ricordiamo infine che la DPIA deve essere rinnovata periodicamente, almeno su base annuale.

La DPIA è uno dei principali documenti dei quali viene chiesta l'esibizione in caso di controllo da parte delle Autorità preposte.

Si resta a disposizione per ogni eventuale chiarimento.

Cordiali saluti

ADOS s.r.l.

(Dott. Simone Sebastiani)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979]

(Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018)

Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

1. 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*".

2. 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).

3. 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.

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): 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).

5. 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 (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7. 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*) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .

8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9. 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*).

10. 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.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.