16 Dicembre 2020
asset/A00_1 /00004762
PROTOCOLLO USCITA
Trasmissione a mezzo posta elettronica, ai sensi dell'art.47 del D. Lgs n. 82/2005

A tutti i dipendenti dell'ASSET
SEDE

OGGETTO: Valutazione d'impatto sulla protezione dei dati personali (cd. DPIA) – Istruzioni operative e modulistica.

La valutazione di impatto sulla protezione dei dati personali, ai sensi dell'art. 35 del Regolamento UE 2016/679[1], costituisce un **processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche** derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

Lo svolgimento della valutazione d'impatto sulla protezione dei dati (DPIA) ha il fine di determinare, in particolare, l'origine, la natura, la particolarità e la gravità del rischio (Considerando n. 84, Reg. UE 2016/679).

In particolare, il suddetto Regolamento UE 2016/679 prevede che "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*" (art. 35, par. 1).

Il Regolamento europeo n. 2016/679 prevede, inoltre, che se il trattamento può comportare un rischio elevato **e non ricorrono ipotesi che lo escludano**, il Titolare del trattamento deve procedere a fare una valutazione d'impatto, previa acquisizione del parere del Responsabile per la Protezione dei Dati (RPD).

Il parere del Responsabile della Protezione dei Dati, previsto dall'art. 35, par. 2, Reg. UE 2016/679, non è vincolante per il titolare, il quale può discostarsi dalle indicazioni ricevute: tuttavia, in casi del genere, il RPD conserva il potere di sorveglianza, ai sensi dell'art. 39, par. 1, lett. b), del Regolamento. In ogni caso, il parere ricevuto dal titolare del trattamento deve essere documentato all'interno della DPIA.

Se, all'esito della DPIA, residua un rischio elevato, il titolare del trattamento deve procedere alla **consultazione preventiva dell'Autorità di Controllo**, ovvero del Garante Privacy, finalizzata all'ottenimento di un parere scritto, ex art. 36 Reg. UE 2016/679.

[1] Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE.

Orbene, sulla base di quanto appena esposto emerge che **la valutazione d'impatto sulla protezione dei dati personali non è obbligatoria per ciascun trattamento, ma solo per quello che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche** (art. 35, par. 1, Reg.).

Il riferimento a «diritti e libertà» degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali, quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

Per l'individuazione dei trattamenti che possono presentare un "rischio elevato", e dunque da sottoporre a DPIA, le Linee Guida dei Garanti privacy europei [2] hanno individuato i seguenti **nove criteri da tenere in considerazione**:

1) trattamenti valutativi o di *scoring*[3], compresa la profilazione[4];

2) decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);

3) monitoraggio sistematico (es: videosorveglianza);

4) trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);

[2] Cfr. Linee Guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento UE 2016/679, adottate il 4 aprile 2017 e modificate il 4 ottobre 2017. Il testo è disponibile al seguente link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[3] In particolare, quando si parla di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione e gli spostamenti dell'interessato. Si pensi, per esempio, ai test genetici effettuati per predire eventuali patologie, alla creazione di profili comportamentali ai fini marketing, ecc.

[4] Per **profilazione** si intende l'insieme delle attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento (segmentazione). L'articolo 4 del nuovo Regolamento europeo definisce la profilazione come "*qualsiasi forma di* ***trattamento automatizzato*** *di dati personali consistente nell'utilizzo di tali dati personali per* ***valutare determinati aspetti personali relativi a una persona fisica****, in particolare per* ***analizzare o prevedere aspetti*** *riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".
Il Considerando 24 specifica ulteriormente che, per stabilire se si è in presenza di profilazione "*è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella* ***profilazione della persona fisica****, in particolare* ***per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali***".
In sintesi, si ha profilazione in presenza di **3 elementi**:
- un trattamento automatizzato;
- eseguito su dati personali;
- con lo scopo di valutare aspetti personali di una persona fisica.

5) trattamenti di dati personali su larga scala;

6) combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);

7) dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);

8) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);

9) trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

Il provvedimento 11 ottobre 2018 del Garante privacy ha introdotto **un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati**, ai sensi dell'art. 35, par. 4, del Reg. UE 2016/679 (cfr. **Allegato 1**).

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati personali, il Gruppo dei Garanti privacy europei raccomanda di **effettuarla comunque**, «*in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento» al fine di «rispettare la legge in materia di protezione dei dati*».

Inoltre, ai sensi dell'art. 39, par. 1, lett. c, Reg. UE 2016/679, il Responsabile della Protezione dei Dati ha l'obbligo di sorvegliare lo svolgimento del procedimento che si conclude con la valutazione d'impatto. Ciò vuol dire che il titolare del trattamento deve aggiornare periodicamente il responsabile delle fasi della procedura, delle scelte poste in essere, dei risultati man mano raggiunti. Ad esempio, se il titolare del trattamento raccoglie le opinioni degli interessati sul trattamento previsto (art. 35, par. 9, Reg.), ne informa il RPD. In questa fase esecutiva, il RPD può offrire supporto, dare indicazioni, esprimere pareri. L'intervento del RPD può anche appuntarsi sui contenuti della valutazione (art. 35, par. 7, Reg.).

Orbene, al fine di accompagnare gli uffici nel complesso processo di valutazione di impatto, il Responsabile per la Protezione dei Dati Personali di ASSET ha predisposto la modulistica allegata alla presente circolare, auspicando che gli uffici la adottino in base alle istruzioni offerte. Si tratta dei seguenti tre moduli:
- Modulo n. 1 - Richiesta del parere al Responsabile per la Protezione dei dati personali – **Allegato 2**;
- Modulo n. 2 - Valutazione d'impatto – **Allegato 3**;
- Modulo n. 3 - Comunicazione degli aggiornamenti al responsabile per la protezione dei dati personali – **Allegato 4**.

La Responsabile per la Protezione dei Dati Personali
Avv. Antonella Caruso

Il Titolare del Trattamento
Direttore Generale
Ing. Raffaele Sannicandro

ALLEGATO 1

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

***CHIARIMENTO INTERPRETATIVO**

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.

ALLEGATO 2

Al Responsabile per la protezione dei dati
dell'ASSET
a.caruso@asset.regione.puglia.it

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)
RICHIESTA DI PARERE AL RESPONSABILE PER LA PROTEZIONE DEI DATI (RPD)
Artt. 35, par. 2, e 39, par. 1, lett. c), del Regolamento generale sulla protezione dei dati[1]

RICHIEDENTE

Nome ……..…….……

Cognome ……..…….…….

Ufficio ……..……...…….

in qualità di[2] ……...…….....

Tel. …… em@il ……

TRATTAMENTO
che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

descrizione del trattamento: ……..……..
……..……..…….
….……...……..……
……...…….……...……
……..……..…….…….
……...……..……...……

INFORMAZIONI *sul trattamento per cui si richiede la DPIA*

Titolare del trattamento …..……...……...

Responsabile del trattamento …..……...……..

Tipologia di dati[3] ……..……

Finalità del trattamento ……..……...……

Mezzi del trattamento ……..……...……...

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

[2] Indicare la qualifica spesa per rappresentare l'ufficio (es. "direttore generale")

[3] Es. dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, etc.

Tipologia di trattamento[4]

☐ incluso nell'elenco del Garante per la protezione dei dati personali contenente i trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati (cfr. Allegato 1 – Circolare ASSET)
(indicare il tipo di trattamento): ……
……
……
……
……
……
……

☐ non incluso nell'elenco del Garante per la protezione dei dati personali contenente i trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati
(indicare i motivi per cui è richiesta la DPIA): ……..
……
……
……
……
……

ULTERIORI INFORMAZIONI*(se ritenute opportune/utili per il parere del RPD)*[5]
……
……
……
……

	Allegati
1	
2	
3	
4	
5	

Luogo e data *Sottoscrizione*
……

[4] Barrare la casella di riferimento

[5] Campo libero. Inserire ogni informazione che si ritenga utile perché il responsabile possa esprimere il proprio parere.

ALLEGATO 3

Al Responsabile per la protezione dei dati
dell'ASSET
a.caruso@asset.regione.puglia.it

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI D.P.I.A.

Artt. 35 del Regolamento generale sulla protezione dei dati[1]

Richiesta *DPIA* prot. n. …….. del ……..	**Aggiornamenti** tot. n. ☐☐☐

La DPIA riguarda: ☐un singolo trattamento ☐un insieme di trattamenti simili

SEZIONE I *– Informazioni sul trattamento*

Titolare del trattamento

Nome ……

Cognome ……..

Ufficio ……..

in qualità di[2] ……...…….....

Tel. …… em@il …….

Responsabile del trattamento …….

Descrizione sistematica dei trattamenti previsti ……..……..
……..……..…….
…..……..……
……..……..……
……..……..…….
Tipologia di dati[3] ……..……
Finalità del trattamento ……..……...……

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

[2] Indicare la qualifica spesa per rappresentare l'ufficio (es. "direttore generale")

[3] Es. dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, etc. [5] Se applicabile

Mezzi del trattamento ……..……..……...
Interesse legittimo perseguito dal titolare del trattamento[5] ……...
SEZIONE II *– Informazioni sui contenuti della DPIA*

Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità: ……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..

Valutazione dei rischi per i diritti e le libertà degli interessati: ……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..

Misure previste per affrontare i rischi[4]: ……
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..
……..……..……..

[4] Includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

……..……..……..…….

SEZIONE III *– Informazioni aggiuntive*

Tipologia di trattamento[5]

☐incluso nell'elenco del Garante per la protezione dei dati personali contenente i trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati (cfr. Allegato 1 Circolare ASSET)

☐*(indicare il tipo di trattamento):* ……..…….
…….
…….
…….

☐non incluso nell'elenco del Garante per la protezione dei dati personali contenente i trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati

☐*(indicare i motivi per cui è stata espletata la DPIA):* ……..
…….
…….
…….

Procedimento di DPIA

☐sono state raccolte le opinioni degli interessati, sul trattamento previsto

☐*(opinioni raccolte*[6]*):* ……..…….
…….
…….
…….

Esecuzione della DPIA

La DPIA è stata affidata a un altro soggetto (interno o esterno all'organizzazione)?

no☐si☐

(*specificare*):……..…….....
….……..…….....
….……..…….....

[5] Barrare la casella di riferimento.

[6] Indicare le persone che sono state consultate, l'opinione che è stata espressa, e ogni altro elemento utile.

SEZIONE IV *– Risultati della valutazione d'impatto*[7]	
☐ *Rischio residuo elevato*	☐ *Rischio residuo non elevato*
Le misure tecniche e organizzative individuate per mitigare l´impatto del trattamento non sono ritenute sufficienti. Il rischio residuale per i diritti e le libertà degli interessati resta elevato	Le misure tecniche e organizzative individuate per mitigare l´impatto del trattamento sono ritenute sufficienti.

E' necessario procedere alla consultazione preventiva del Garante per la protezione dei dati personali, ai sensi dell'art. 36 GDPR

ULTERIORI INFORMAZIONI*(se ritenute opportune/utili)*

……
……
……
……

	Allegati	**data**
1	Richiesta di parere al responsabile per la protezione dei dati	
2	Parere del responsabile per la protezione dei dati	
3	*(eventualmente)* Comunicazioni di aggiornamento rese al RPD	
4		
5		

Luogo e data *Sottoscrizione*

……

[7] Barrare la casella corrispondente. Si ricorda che il titolare deve procedere al riesame sulla conformità del trattamento alla DPIA in caso di variazioni del rischio (cfr. art. 35, par. 11, GDPR).

ALLEGATO 4

Al Responsabile per la protezione dei dati
dell'ASSET
a.caruso@asset.regione.puglia.it

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

AGGIORNAMENTO SUL CORSO DEL PROCEDIMENTO[1]

Artt. 35, par. 2, e 39, par. 1, lett. c), del Regolamento generale sulla protezione dei dati[3]

DPIA prot. n. …..…….. del ……...……	☐ **Aggiornamento** n.

INFORMAZIONI SUL PROCEDIMENTO

Richiedente….……..…….....

Titolare del trattamento …..……..……...

Responsabile del trattamento …..……..……..

Data della richiesta di DPIA ……..…….

Contenuti dell'aggiornamento

sono state raccolte le opinioni degli interessati, sul trattamento previsto

(opinioni raccolte[2]): ……..…….

…….

…….

…….

…….

…….

[1] Il RPD deve sorvegliare lo svolgimento del procedimento che si conclude con la valutazione d'impatto. Il titolare del trattamento, pertanto, deve aggiornare periodicamente il responsabile delle fasi della procedura, delle scelte poste in essere, dei risultati man mano raggiunti. [3] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[2] Indicare le persone che sono consultate, l'opinione che è stata espressa, e ogni altro elemento utile

Contenuti dell'aggiornamento

□ sono sopravvenute le seguenti modifiche, rispetto alle informazioni originariamente comunicate:

(indicare in modo specifico[3]): ……..
……
……
……
……
……

□ sono subentrate variazioni del rischio rappresentato dalle attività relative al trattamento.

(specificare[4]): ……
……
……
……
……
……

□ altre informazioni

(indicare in modo specifico): ……
……
……
……
……
……

	Allegati
1	
2	
3	
4	
5	

Luogo e data	*Sottoscrizione*
……	

[3] Indicare circostanze che sono cambiate rispetto a come rappresentate nella originaria richiesta di DPIA: es., mezzi del trattamento, qualità e quantità dei dati, etc.

[4] Indicare se vi sono state modifiche sul rischio originariamente considerato