Allegato n. 4

CAMERA DI COMMERCIO
DEL SUD EST SICILIA

Camera di commercio, industria,artigianato e agricoltura del Sud Est Sicilia

Procedura per la predisposizione di una valutazione di impatto sulla protezione dei dati personali (DPIA)

ai sensi del Regolamento UE 679/2016

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente **procedura** è disciplinare il processo per eseguire la "valutazione di impatto sulla protezione dei dati" (DPIA) qualora si renda necessaria per un trattamento, o un insieme di trattamenti simili, effettuato dalla Camera del Sud est Sicilia al fine di valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli).

L'obbligo di condurre una DPIA si colloca nel contesto del più ampio obbligo imposto ai titolari di **gestire correttamente i rischi connessi al trattamento di dati personali**.

Si tenga conto inoltre che:

a) la realizzazione di una DPIA è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche";

b) il GDPR prevede che la DPIA debba essere effettuata del **titolare del trattamento** (art. 35, par. 1 e Considerando 84), tuttavia, la valutazione può essere effettuata anche da altro soggetto, interno o esterno all'organizzazione, fermo restando che al titolare spetta la responsabilità ultima di tale compito;

c) nei rapporti di **contitolarità** ciascun contitolare attua la sua procedura per quanto attiene al trattamento dei dati che gli compete.

La presente procedura è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i Dirigenti, Responsabili delle Unità organizzative, funzionari o, comunque, referenti delle Aree/Uffici/Servizi della Camera di Commercio del Sud est Sicilia.

RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Valutazione d'impatto sulla protezione dei dati (art. 35 e 36 del GDPR e Considerando 84, 89-96);
2. WP248 rev. 01, 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 riemesse il 4 ottobre 2017;
3. Provvedimento del Garante per la protezione dei dati personali n. 467 dell'11 ottobre 2018 (Pubblicato sulla G.U. n. 269 del 19 novembre 2018) contenente l'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 Regolamento (UE) n. 2016/679.

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (*General Data Protection Regulation*)
Codice	D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. n. 101/2018
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) – EDPB (European Data Protection Board)

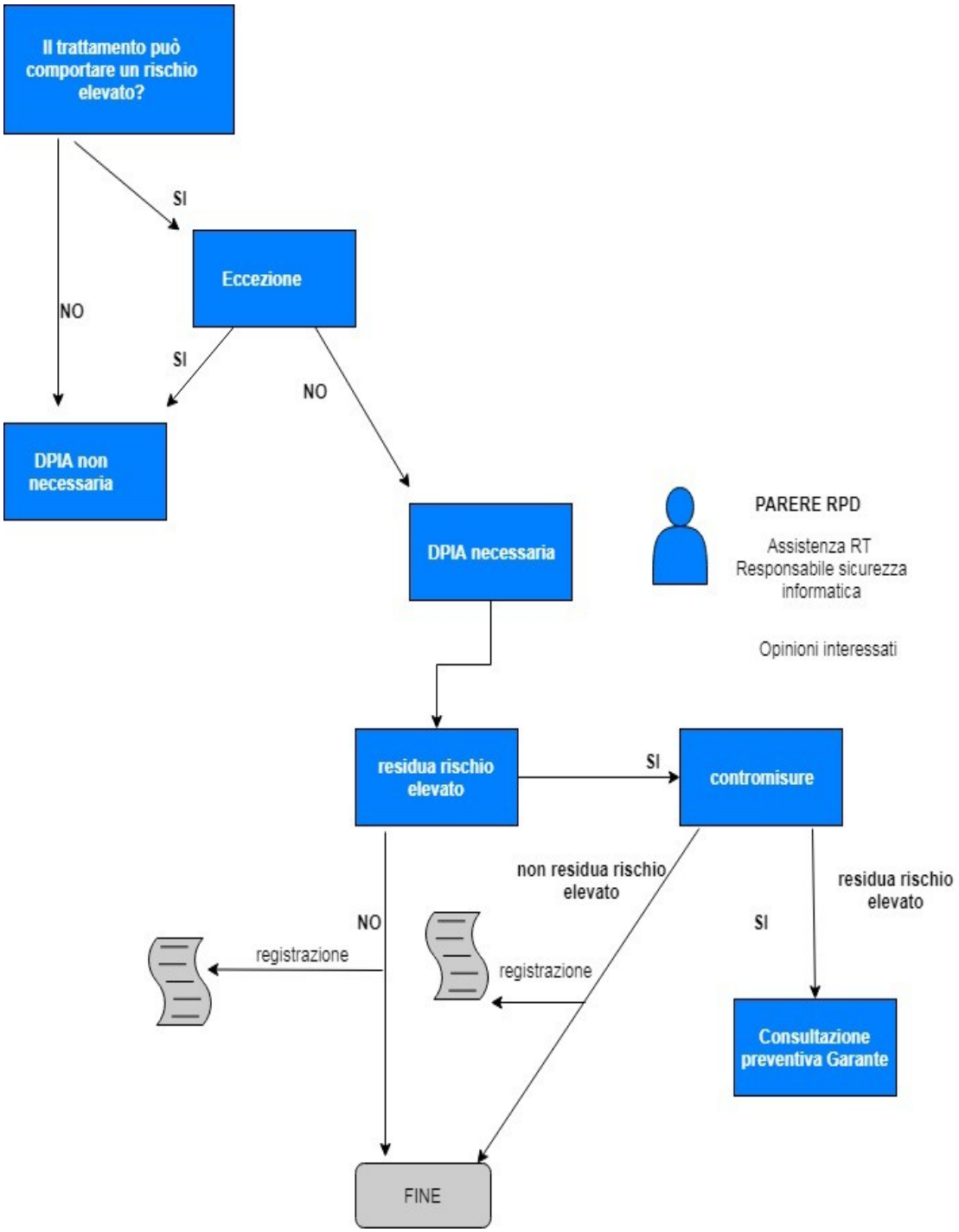
RPD/DPO	Responsabile della protezione dei dati (Data Protection Officer)
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR
SG	Segretario Generale della Camera
DPIA	Data Protection Impact Assessment (Valutazione d'impatto sulla protezione dei dati)
RT	Responsabile del Trattamento

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione

FASI DEL PROCESSO

La gestione di una DPIA può riassumersi nelle fasi di seguito rappresentate.



TRATTAMENTI SOGGETTI A DPIA

Il GDPR non richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati per tutti i trattamenti che possono presentare rischi per i diritti e le libertà delle persone fisiche. La realizzazione di una DPIA è obbligatoria soltanto qualora il trattamento **"possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche"** (art. 35, par. 1).

Secondo il WP 29, il Regolamento generale sulla protezione dei dati prevede che i titolari del trattamento attuino misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto regolamento, tenendo conto tra l'altro dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.

Lo stesso art. 35 fornisce, a titolo esemplificativo, **tre casi** nei quali il trattamento può presentare rischi elevati, ossia:

- ✓ valutazione sistematica e globale di **aspetti personali relativi a persone fisiche**, basata su un **trattamento automatizzato**, compresa la **profilazione**, e sulla quale si fondano **decisioni che hanno effetti giuridici** o incidono in modo analogo significativamente su dette persone fisiche;
- ✓ **trattamento, su larga scala**, di categorie **particolari** di dati personali (art. 9 GDPR) o di dati relativi a **condanne penali e a reati** (art. 10)
- ✓ **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico, in particolare se effettuata mediante dispositivi optoelettronici

Anche le linee guida wp248 rev.01, adottate dal gruppo di lavoro articolo 29 (in seguito wp248) individuano **nove criteri** che devono essere considerati al fine di determinare i trattamenti soggetti a DPIA. Sul punto è intervenuto anche il Garante che, con provvedimento n. 467 dell'11 ottobre 2018 ha disposto **un elenco** delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto.

Nell'Allegato "A", riportato in questo documento, è riassunto in maniera ragionata il contenuto delle tre fonti disciplinari sopra menzionate, e rappresenta lo strumento che dovrà essere utilizzato a monte dell'intera procedura, al fine di **identificare**, tra tutti i trattamenti mappati nel "Registro dei trattamenti della Camera di commercio del Sud est Sicilia", quelli che dovranno essere sottoposti ad una DPIA.

Resta fermo che vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale allegato, ma che presentano tuttavia rischi altrettanto elevati (specialmente i trattamenti che prevedono l'uso di nuove tecnologie). Di conseguenza, anche questi trattamenti devono essere soggetti alla DPIA.

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, la DPIA dovrà essere effettuata comunque.

Si ricorda inoltre che:

a) il Responsabile esterno del trattamento deve assistere il Titolare nell'effettuazione della DPIA "tenendo conto della natura del trattamento e delle informazioni in possesso del responsabile del trattamento" (art. 28, par. 3, lett. f));

b) tra i compiti affidati al RPD, ex art. 39, par. 1, lett. c) del GDPR, vi rientra anche:

- la consultazione con il Titolare sullo svolgimento della DPIA (art. 35, par. 2, GDPR);
- fornire, *se richiesto dal Titolare*, un parere in merito alla DPIA;
- sorvegliare lo svolgimento della DPIA ai sensi dell'art. 35[1].

1 La richiesta del titolare può riguardare il parere sulla DPIA ma non la sorveglianza della stessa. I compiti di sorveglianza competono infatti al RPD in forza dell'art. 39, par. 1, lett. b), del GDPR.

ECCEZIONI

La valutazione d'impatto sulla protezione dei dati **non** è richiesta nei seguenti casi:

1. quando il trattamento non presenta "un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, par. 1, del GDPR);

2. quando è già stata effettuata una DPIA con riferimento a **trattamenti simili** che presentano rischi elevati analoghi (art. 35, par. 1, del GDPR);

3. quando le tipologie di trattamento sono state **verificate da un'autorità di controllo** prima del maggio 2018 in condizioni specifiche che non sono cambiate (wp248);

4. qualora un trattamento (effettuato per adempiere un obbligo di legge, ovvero necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare) trovi una **base giuridica** nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (art. 35, par. 10, del GDPR);

5. qualora il trattamento sia incluso nell'**elenco facoltativo** (stabilito dal Garante) delle tipologie di trattamento per le quali non è richiesta alcuna DPIA (art. 35, par. 5, del GDPR).

QUANDO SI EFFETTUA LA DPIA

La DPIA deve essere effettuata **prima** di procedere al trattamento, già dalla fase di **progettazione** dello stesso, in coerenza con i principi di *privacy by design* e *privacy by default*, per determinare se il trattamento deve prevedere misure appropriate in grado di mitigare i rischi.

Seppure il Regolamento evidenzi l'applicazione della valutazione di impatto per i nuovi trattamenti, è necessario valutare anche i **trattamenti in corso avviati prima del 25 maggio 2018** arrivando comunque a determinare la loro conformità al GDPR e la necessità o meno di effettuare una DPIA.

Considerato che le operazioni di trattamento dei dati personali possono evolversi rapidamente e che potrebbero emergere nuove vulnerabilità, la valutazione d'impatto sulla protezione dei dati **va riesaminata e rivalutata con regolarità**.

SOGGETTI CHE EFFETTUANO E INTERVENGONO NELLA DPIA

Il GDPR prevede che la DPIA debba essere effettuata del **titolare del trattamento** (art. 35, par. 1 e Considerando 84), tuttavia, la valutazione può essere effettuata anche da altro soggetto, interno o esterno all'organizzazione, fermo restando che al titolare spetta la **responsabilità ultima** di tale compito.

Nell'ambito della Camera di Commercio del Sud est Sicilia la DPIA viene effettuata dal Delegato del Titolare.

Come indicato in precedenza il **responsabile per la protezione dei dati** (RPD) svolge un ruolo fondamentale assistendo il Delegato del titolare nello svolgimento della DPIA.

In ossequio al principio di "protezione dei dati fin dalla progettazione" (*privacy by design*), l'art. 35, par. 2, prevede in modo specifico che il titolare "*si consulta*" con il RPD quando svolge una DPIA. A sua volta, l'art. 39, par. 1, lett. c), affida al RPD i compiti di "*fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati"* e di *"sorvegliarne lo svolgimento ai sensi dell'articolo 35*".

Conseguentemente la Camera di commercio del Sud est Sicilia consulta il RPD sulle seguenti tematiche:

- se condurre o meno una DPIA;

- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e le libertà delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno;
- se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;
- [effettuazione della consultazione preventiva al Garante, di cui all'art. 36 del GDPR)].

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

Anche l'**Amministratore di sistema** ovvero il **responsabile della sicurezza dei sistemi informativi**, e/o l'ufficio competente per detti sistemi, forniscono supporto al titolare ed al RPD per lo svolgimento della DPIA.

Un ruolo determinante nella realizzazione di una DPIA è rivestito inoltre dal **responsabile del trattamento**, cioè dal soggetto che tratta i dati personali per conto del titolare. Qualora il trattamento venga eseguito in toto o in parte da un RT, quest'ultimo deve **assistere** il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie (conformemente all'art. 28, par. 3, lett. f)).

Infine, l'art. 35, par. 9, del GDPR, prevede, **se del caso**, che il titolare del trattamento raccolga le **opinioni degli interessati** (o dei loro rappresentanti) sul trattamento, **fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti**. La norma sembra lasciare libero ogni titolare del trattamento, nella valutazione **sul se** e **sul come** raccogliere le opinioni in parola. Sul punto, il wp248 aggiunge tuttavia che il titolare del trattamento deve **giustificare** (e documentare) la mancata raccolta delle opinioni degli interessati, qualora decida che ciò non sia appropriato, ad esempio qualora ciò comporterebbe la riservatezza dei piani economici dell'impresa o **sarebbe sproporzionato o impraticabile**.

CONSULTAZIONE DELL'AUTORITA' GARANTE

Qualora, all'esito di una DPIA, i rischi siano considerati sufficientemente attenuati dal titolare, il trattamento può procedere senza necessità di consultare l'Autorità di controllo. Questo è possibile anche a seguito dell'applicazione di idonee contromisure adatte a mitigare l'impatto o la gravità dei rischi per la libertà e i diritti degli interessati.

Diversamente, nei casi in cui il titolare del trattamento non riesca a gestire in maniera sufficiente i rischi individuati (ossia i rischi residui rimangono elevati), questi, qualora voglia procedere con il trattamento, deve prima consultare il Garante, ex art. 36 del GDPR.

Inoltre, il titolare del trattamento deve consultare il Garante qualora il diritto italiano prescriva che i titolari consultino l'autorità di controllo e ne ottengano l'autorizzazione preliminare, in relazione a trattamenti per l'esecuzione di un compito di interesse pubblico (art. 36, par. 5, del GDPR)[2].

FASI DELLA PROCEDURA

Per **tutti** i trattamenti inseriti nel "Registro dei trattamenti della Camera di Commercio del Sud est" e per i quali lo stesso Ente sia titolare, deve essere valutato se possono presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche. Sono esclusi i trattamenti che costituiscono specifica **eccezione** in conformità a quanto sopra indicato.

2 V., per es., l'art. 110, comma 1, terzo paragrafo, del D.Lgs. n. 196/2003.

Il Delegato del titolare utilizzerà la checklist di dettaglio di cui all'allegato "A" alla presente procedura (resta fermo che vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale allegato, ma che presentano tuttavia rischi altrettanto elevati. Di conseguenza, anche questi trattamenti devono essere soggetti alla DPIA).

Ad esito dell'analisi:

A) nel caso in cui il trattamento **non presenti** un rischio elevato per i diritti e le libertà delle persone fisiche, non si procederà con la DPIA. Tale informazione deve essere annotata nel Registro dei trattamenti, ovvero in altro documento, in modo da poter dimostrare di aver proceduto alla realizzazione di una valutazione preventiva completa e conforme al GDPR;

B) nel caso in cui sia stato valutato che il trattamento **presenti** un rischio elevato per i diritti e le libertà delle persone fisiche, si procederà con la DPIA, utilizzando lo strumento applicativo realizzato allo scopo (riportato nell'Allegato "B"), e procedendo quindi alla redazione di una scheda che, al termine del processo, dovrà essere salvata in formato non modificabile e firmata digitalmente dal Delegato del titolare che esegue la DPIA e dal RPD che esprime il proprio parere. Gli estremi della DPIA devono essere annotati nel Registro dei trattamenti.

Ove si verificassero **conflitti decisionali** rispetto alla scelta di procedere o meno alla DPIA, dovranno essere specificate le responsabilità finali della decisione, il parere del RPD, ovvero i motivi per i quali lo stesso non sia stato consultato.

DESCRIZIONE DEL TRATTAMENTO

Il primo passaggio della valutazione d'impatto ha natura prettamente descrittiva, essendo teso a rappresentare in modo dettagliato e puntuale il trattamento nel suo insieme.

La compilazione della prima scheda soddisfa e amplia il contenuto dell'art. 35, par. 7, lett. a), del GDPR: "*La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento*".

NECESSITA' E PROPORZIONALITA'

Il secondo passaggio consiste nel valutare la **necessità** e la **proporzionalità** dei trattamenti in relazione alle finalità, tenendo conto dei criteri individuati nell'allegato 2 del WP248. Si tratta di criteri che, se soddisfatti o meno, possono incidere indirettamente anche sul rischio, andando a mitigarne (o ad ampliarne se non soddisfatti) gli **impatti** (la gravità).

A titolo esemplificativo, il rischio che i dati personali possano essere non aggiornati od obsoleti, potrebbe essere mitigato dalla possibilità data agli interessati di esercitare liberamente, agevolmente, e in qualsiasi momento, i diritti di rettifica e/o di cancellazione (artt. 16 e 17 del GDPR).
Per questa ragione, la scheda prevede, tra gli altri, l'obbligo di risposta alle seguenti domande:
- I dati personali sono esatti e aggiornati?
- E' data la possibilità agli interessati di esercitare i loro diritti?

Questa scheda assolve al precetto di cui all'art. 35, par. 7, lett. b), del GDPR: "*La valutazione contiene almeno: (…) b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità*".

ACCESSO – MODIFICA – PERDITA

Si tratta, rispettivamente, di tre schede predisposte per dare attuazione all'art. 35, par. 7, lett. c), del GDPR: "*La valutazione contiene almeno: (…) c) una valutazione dei rischi per i diritti e le libertà degli interessati* […]".

Per "**rischio**" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di **gravità** e **probabilità**.

La "**gestione dei rischi**", invece, è l'insieme delle attività dell'ente, coordinate, e volte a indirizzare e controllare l'ente in relazione ai rischi.

Infine, posto che il rischio non si riferisce al titolare ma al soggetto interessato, la **valutazione complessiva del rischio (VCR)** deve contemplare, tanto gli "aspetti che riguardano la sicurezza del trattamento", quanto "gli effetti complessivi del trattamento".

Gli aspetti che riguardano la **sicurezza del trattamento** sono inquadrabili nella:

1. **RISERVATEZZA** (divulgazione, accesso): riclassificato nell'applicativo sinteticamente in "rischio di accesso illegittimo ai dati".
2. **INTEGRITÀ** (alterazione): riclassificato nell'applicativo in "rischio di modifica indesiderata dei dati".
3. **DISPONIBILITÀ** (distruzione, indisponibilità, perdita): riclassificato nell'applicativo sinteticamente in "rischio di perdita indesiderata dei dati".

Per ciascun rischio così individuato deve essere determinata la **probabilità** che lo stesso si realizzi, misurata utilizzando i seguenti valori/frequenze:

- (0) nessuna probabilità;
- (1) improbabile;
- (2) poco probabile;
- (3) probabile;
- (4) molto probabile;
- (5) altamente probabile.

In questa fase dovranno quindi essere individuati i possibili rischi "patologici" incombenti sui dati personali oggetto di trattamento, cioè, in sostanza, **il grado di probabilità che si verifichino "violazioni dei dati",** come definite all'art. 4 del GDPR ("la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati").

Compiuta questa valutazione preliminare sugli aspetti che riguardano la sicurezza del trattamento, segue una seconda fase che riguarda la **gravità del danno** (l'impatto), dove, nella prospettiva dell'interessato, occorre valutare i **rischi per i diritti e le libertà delle persone fisiche**, quali, ad esempio, i danni alla reputazione, discriminazione, furto d'identità, perdite finanziarie, perdita di controllo dei dati, impossibilità di esercitare diritti, così come individuati nel Considerando 75 del GDPR.

La **gravità** (impatto) sui diritti e le libertà delle persone fisiche, viene misurata secondo i valori/importanza sotto riportati:

- (0) nessun impatto;
- (1) marginale;
- (2) minore;
- (3) soglia;
- (4) serio;
- (5) superiore.

Solo a valle di questa **duplice valutazione**, comprendente la casistica patologica del *data breach*, ma anche e, soprattutto, il potenziale impatto negativo sui diritti e le libertà delle persone di quel trattamento in sé, che sarà possibile determinare la **Valutazione Complessiva del Rischio (VCR)** e, conseguentemente, procedere alla individuazione delle misure di mitigazione più o meno mirate ed efficaci.

MISURE

E' un passaggio nodale, dove, anche alla luce delle risultanze delle schede precedenti, dovranno essere individuate e descritte tutte le **misure** previste per affrontare/mitigare i rischi.

Si dovrà quindi provvedere a indicare su quale dei tre rischi (acceso, modifica e perdita) la singola misura incide.

La scheda contiene anche una legenda (elenco non esaustivo) delle principali misure (applicate ai dati, generali di sicurezza dei sistemi, organizzative, etc.), adottabili da una struttura più o meno articolata.

La scheda soddisfa il dettato dell'art. 35, par. 7, lett. d), del GDPR: "*La valutazione contiene almeno: (…) 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 presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione*".

A tale proposito, in caso di trattamento effettuato da un **responsabile del trattamento**, occorre acquisire le informazioni necessarie a valutare l'adeguatezza delle misure tecniche e organizzative adottate. Il Delegato del titolare che esegue la DPIA può farsi assistere dal responsabile della sicurezza dei sistemi informativi.

VALUTAZIONE FINALE

E' la scheda conclusiva, che dovrà essere stampata in formato non modificabile (PDF) e firmata digitalmente dal soggetto che effettua la DPIA e dal RPD.

Detta scheda, si compone di **quattro sezioni** che si compilano automaticamente valorizzando le schede precedenti:

1. **Panoramica dei rischi**
2. **Panoramica della necessità e della probabilità**
3. **Panoramica delle misure**
4. **Esito finale della DPIA**: restituisce a sua volta tre tipologie di risultati generati automaticamente da una serie di algoritmi che tengono conto dei valori delle tre sezioni precedenti e di un valore di rischio accettabile precedentemente definito in associazione tra il titolare del trattamento e il RPD:
   a. l'esito generale della DPIA: può essere positivo (luce verde, si può procedere con il trattamento), ovvero negativo (luce rossa, cioè il trattamento è altamente sconsigliato);
   b. la data entro cui dovrà essere effettuata la revisione della valutazione di impatto;
   c. l'Alert sulla presenza di particolari categorie di dati, ovvero di soggetti vulnerabili che richiedono una specifica attenzione di trattamento.

Sono inoltre presenti **tre sezioni** <u>che dovranno, invece, essere valorizzate dal soggetto che effettua la valutazione di impatto</u>:

- l'individuazione del soggetto che ha effettuato la Valutazione di impatto (nome, cognome e ruolo ricoperto all'interno dell'ente);
- il parere del Responsabile della protezione dei dati;
- accoglimento o meno del parere del RPD. In caso di non accoglimento ne andranno specificate le ragioni.

CHIUSURA DELLA PROCEDURA

All'esito del processo sopra illustrato si potranno presentare le seguenti alternative:

A. qualora il valore di rischio sia compreso entro la soglia di accettabilità (**esito positivo**) il trattamento potrà essere definito sufficientemente sicuro e si potrà procedere con il trattamento;
B. nel caso in cui il valore di rischio residuo risulti sopra la soglia di accettabilità (**esito negativo**) si dovrà procedere a rivedere le contromisure applicate alzando il livello di implementazione di quelle esistenti oppure introducendone di nuove. In tal caso il valore di rischio dovrà essere ricalcolato

(predisponendo una nuova scheda DPIA) ottenendo quindi un nuovo valore a seguito dell'applicazione delle nuove contromisure;

C. ove il valore di rischio residuo risulti sopra la soglia di accettabilità (**esito negativo**) e il titolare del trattamento non sia in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile, il titolare del trattamento (o suo delegato), prima di procedere al trattamento, deve consultare il Garante (secondo le modalità descritte nell'art. 36 del GDPR). Tale adempimento deve essere considerato parte integrante del processo di DPIA. Alternativamente, il titolare potrà semplicemente scegliere di non effettuare il trattamento in questione.

CONSULTAZIONE PREVENTIVA

Ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare il Garante.

Nella comunicazione al Garante, il titolare indica:

a. ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;
b. le finalità e i mezzi del trattamento previsto;
c. le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
d. i dati di contatto del responsabile della protezione dati;
e. la valutazione d'impatto eseguita;
f. ogni altra informazione richiesta dal Garante.

L'art. 36, par. 2, del GDPR, prevede che "(…) qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione".

Al riguardo, l'art. 154, comma 5, del D.Lgs. n. 196/2003, stabilisce che "Fatti salvi i termini più brevi previsti per legge, il parere del Garante, anche nei casi di cui all'art. 36, par. 4, del Regolamento, è reso nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate".

REVISIONE DELLA DPIA

La DPIA non deve intendersi come un'attività da effettuarsi *una tantum*, ma è un processo che deve essere ciclicamente revisionato tutte le volte che si renda necessario in base ai cambiamenti interni o esterni che si dovessero presentare al trattamento.
La scheda finale dello strumento applicativo, a seconda delle diverse tipologie di trattamento e dei risultati generati dall'algoritmo, individua una revisione semestrale, ovvero annuale, indicando la data entro cui dovrà avvenire la **revisione**.

In ogni caso, nel caso di modifiche importanti a trattamenti esistenti, si deve prevedere sempre una revisione della DPIA.

A seguire alcuni esempi di modifiche alle attività di trattamento, rischi connessi e cambiamenti nel contesto organizzativo o sociale, che devono indurre a una revisione della DPIA:

Cambiamento sulle attività di trattamento, in termini di:
- Contesto;
- Finalità del trattamento;
- Tipologia di dati personali trattati;
- Destinatari (ad eccezione di quelli che rientrano nella definizione di «terzo» ai sensi dell'art. 4, num. 10), del GDPR);
- Modalità di raccolta dei dati personali;
- Trasferimento di dati all'estero.

Modifica ai rischi con impatto sui diritti degli interessati derivati da:
- Presenza di nuove minacce;
- Modifica ai sistemi informativi a supporto del trattamento;
- Soppressione/modifica di contromisure esistenti.

ALLEGATO A – CHECK LIST

GDPR	WP248 (obbligatoria se sono soddisfatti almeno due criteri)	Garante (Allegato 1 provv. 467 dell'11.10.2018) [doc.web n. 9058979]
	1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "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" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;	**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".
(articolo 35, paragrafo 3, lettera a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;	2. **Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente**: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico;	**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).
(articolo 35, paragrafo 3, lettera c) la sorveglianza sistematica **su larga scala** di una zona	**3. monitoraggio sistematico:** trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza	**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,

GDPR	WP248 (obbligatoria se sono soddisfatti almeno due criteri)	Garante (Allegato 1 provv. 467 dell'11.10.2018) [doc.web n. 9058979]
accessibile al pubblico	sistematica su larga scala di una zona accessibile al pubblico" (art. 35, par. 3, lett. c)). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);	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, ecc.
(articolo 35, paragrafo 3, lettera b) il trattamento, **su larga scala**, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;	**4. Dati sensibili o dati aventi carattere altamente personale:** questo criterio include categorie particolari di dati personali così come definite all'articolo 9, nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Al di là di queste disposizioni del GDPR, alcune categorie di dati possono aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati sensibili perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche, la cui riservateza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad es. i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione), oppure perché la violazione di tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzo. Il fatto che i dati personali siano di dominio pubblico può essere preso in considerazione nella DPIA qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica,	**4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP248, 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).

GDPR	WP248 (obbligatoria se sono soddisfatti almeno due criteri)	Garante (Allegato 1 provv. 467 dell'11.10.2018) [doc.web n. 9058979]
	diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone.	
	5. Trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento.	**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**. Creazione di corrispondenze o combinazione di insiemi di dati**, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;	**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.**
	7**. Dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei	**6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili** (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

GDPR	WP248 (obbligatoria se sono soddisfatti almeno due criteri)	Garante (Allegato 1 provv. 467 dell'11.10.2018) [doc.web n. 9058979]
	loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire liberamente e consapevolmente al trattamento dei loro dati) i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo, anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento.	
	8. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi.	**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 prossimitaà come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
	9. Quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò	

GDPR	WP248 (obbligatoria se sono soddisfatti almeno due criteri)	Garante (Allegato 1 provv. 467 dell'11.10.2018) [doc.web n. 9058979]
	è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.	
		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.

ECCEZIONI	
GDPR	**WP248**
(**articolo 35, paragrafo 10)** Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento e soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, **e** sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.	Qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico **o** sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
(articolo 35, paragrafo 1) 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.	Quanto il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, par. 1)
(articolo 35, paragrafo 1) Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.	Quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 1);
Considerando 171 Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.	Quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate (cfr. III.C).
(articolo 35, paragrafo 5) L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.	Qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, par. 5).