

Valutazione d'impatto sulla protezione dei dati DPIA

NOME DEL PROGETTO:	
DESCRIZIONE DEL PROGETTO:	

Responsabile elaborazione DPIA:	nome	Posizione:	
---------------------------------	------	------------	--

Sommario

Sezione 0 - Verifica preliminare di applicabilità della DPIA, in conformità all’articolo 35 del regolamento generale	1
Sezione 1 - Avvio della valutazione	2
Sezione 2 - Impostazione dell’analisi di rischio preliminare	3
Sezione 3 - Esito dell’analisi preliminare dei rischi	6
Sezione 4 - Preparazione per la fase di consultazione ed analisi	7
Sezione 5 - Consultazione	9
Sezione 6 - Congruità con altre leggi, codici o regolamenti afferenti alla protezione dei dati.....	10
Sezione 7 - Contenuti analitici della DPIA	11
Sezione 8 - Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati -art 35	13
Sezione 9 - Approvazione della DPIA	14
Sezione 10 - Attivazione del trattamento	15
Appendice A - Lista di controllo della congruità del trattamento previsto con le esigenze di protezione dei dati	16
Appendice B - Tabella dei rischi afferenti alla DPIA	18

Sezione 0 - Verifica preliminare di applicabilità della DPIA, in conformità all'articolo 35 del regolamento generale

Verificare se il trattamento coinvolto, dopo essere stato assoggettato all'analisi di rischio, può ricadere in uno dei casi previsti, per i quali è obbligatoria la conduzione di una DPIA¹

- Trattamenti sistematici ed estensivi di valutazione di aspetti personali dell'interessato, basati su sistemi automatizzati, inclusa la profilazione, i cui esiti portino a decisioni che possono avere effetti legali diretti ed indiretti sull'interessato-articolo 35, paragrafo 2^a
- Trattamento di dati afferenti a profili penali e giudiziari come illustrato nell'articolo 9;
- monitoraggio automatico di aree pubbliche, su larga scala²
- altre attività di trattamento che siano inseriti nell'elenco pubblico dell'autorità garante nazionale, e che richiedono specificamente allo sviluppo di un data protection impact assessment-articolo 35.
- trattamenti in cui una violazione dei dati può avere un impatto negativo sulla protezione dei dati stessi, nonché la riservatezza e i diritti o i legittimi interessi degli interessati coinvolti
- attività di trattamento che non rientra nei casi precedenti, ma per le quali il data controller redatto processo ritengono comunque sia appropriato svolgere una data protection impact assessment

Data di avvio della DPIA:

¹ nota: è possibile che un trattamento comporti numerosi riferimenti incrociati si faccia anche attenzione al fatto che può essere raccomandata la conduzione di una valutazione di impatto, anche se il trattamento in questione non risulta fra quelli per i quali tale valutazione sia obbligatoria. La presenza di questa valutazione, anche in attività di trattamento non obbligatorie, rappresenta una garanzia per tutti i soggetti coinvolti.

² nota: fare particolare attenzione a impianti di videosorveglianza di grandi dimensioni, in porti, aeroporti, parchi, abiti cittadini in genere

Sezione 1 - Avvio della valutazione

1.1 traccia del progetto³

1.1 traccia del progetto ³

1.2 valutazione preliminare dell'utilizzo dei dati⁴

1.2.2 Come i dati verranno raccolti?

1.2.2 Come i dati verranno raccolti?

1.2.3 Chi avrà accesso ai dati? ⁵

1.2.3 Chi avrà accesso ai dati? ⁵

1.2.4 In che modo i dati verranno trasferiti a soggetti terzi?

1.2.4 In che modo i dati verranno trasferiti a soggetti terzi?

1.2.5 Come i dati verranno archiviati, aggiornati ed eliminati quando non più necessari?⁶

1.2.5 Come i dati verranno archiviati, aggiornati ed eliminati quando non più necessari? ⁶

1.3 analisi preliminare dei soggetti coinvolti ⁷

1.3 analisi preliminare dei soggetti coinvolti ⁷

1.4 analisi di contesti precedenti e simili ⁸

1.4 analisi di contesti precedenti e simili ⁸

Sezione 1 completata da:		Data:	
--------------------------	--	-------	--

³ Nota: esaminate le finalità del progetto in modo da esser certi di conoscere gli obiettivi e l'impatto potenziale. Probabilmente esiste già un documento introduttivo cui fare riferimento. Se no, coinvolgere il personale e tutti i terzi coinvolti nel progetto

⁴ Nota: rispondete alle domande seguenti in modo che vi sia una chiara comprensione di come le informazioni verranno utilizzate, chi le userà eccetera. Ricordatevi che sono i dati personali di specifici soggetti che devono attrarre la vostra attenzione. Se non siete in grado di rispondere adesso a tutte le domande, scrivete almeno ciò che già conoscete

⁵ Nota: descrivete tutti i soggetti cui i dati potrebbero essere trasferiti e analizzatene il livello di accesso. Potrebbe essere utile creare un diagramma di flusso che illustri come i dati vengono trasferiti dal punto di raccolta ad altri soggetti coinvolti

⁶ Nota: attenzione al fatto che queste domande fanno riferimento a tutti coloro che hanno accesso ai dati. Attenzione particolare alle normative europee per cancellare dati cartacei ed informatici

⁷ Nota: questa analisi deve fare riferimento a tutti coloro che sono coinvolti nel progetto ed anche a coloro che potrebbero essere coinvolti, seppure di riflesso. È meglio compilare, questo punto, una lista la più ampia possibile, che potrà essere ridotta successivamente, quando l'indagine diventerà sempre più focalizzata

⁸ Nota: in questa fase è opportuno raccogliere informazioni su progetti precedenti, di natura similare, sviluppatisi all'interno, sia all'esterno dell'ente. Questa indagine può essere utile per acquisire preziose informazioni su problemi e soluzioni incontrate in precedenza. C'è sempre da imparare dalle esperienze altrui

Sezione 2 - Impostazione dell'analisi di rischio preliminare⁹

Le domande che seguono permettono di assumere una decisione circa il fatto che sia o meno appropriata lo sviluppo di una DPIA e il livello di approfondimento della stessa, anche in casi dove tale DPIA non è obbligatoria

2.1 Tecnologie utilizzate

2.1.1 in questo progetto verranno utilizzate nuove tecnologie informatiche che potrebbero avere un significativo potenziale di violazione della protezione dei dati personali e riduzione del livello di protezione dei dati, che bisogna garantire agli interessati?

2.2 Metodi di identificazione

2.2.1 verranno utilizzati nuovi metodi di identificazione dei dati o verranno riutilizzati identificatori già esistenti ed in uso?

2.2.3 verranno utilizzati nuovi o significativamente modificati requisiti di autentica di identità, che possono risultare intrusivi od onerosi?

2.3 Coinvolgimento di altre strutture

2.3.1 Questa iniziativa di trattamento coinvolge altre strutture, sia pubbliche, sia private, sia appartenenti a settori non-profit e volontari?

2.4 Modifiche alle modalità di trattamento dei dati

2.4.1 Questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di trattamento dei dati personali, che potrebbero destare preoccupazioni nell'interessato? ¹⁰

2.4.2 i dati personali, afferenti ad un interessato, già presenti in un esistente data base, verranno assoggettati a nuove o modificate modalità di

⁹ nota: una analisi di rischio è sempre necessaria, per decidere se una DPIA è obbligatoria o raccomandata

¹⁰ nota: queste modifiche potrebbero riguardare le origini razziali ed etniche, le opinioni politiche, i dati sanitari, la vita sessuale, trascorsi giudiziari nonché informazioni finanziarie, che potrebbero consentire un furto di identità

trattamento?

2.4.3 i dati personali, afferenti ad un gran numero di interessati, verranno assoggettati a nuove o significative modifiche delle modalità di trattamento?

2.4.4 questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di consolidamento, interscambio, riferimenti incrociati, abbinamento di dati personali, provenienti da più sistemi di trattamento ?

2.5 Modifiche alle procedure di trattamento dei dati

2.5.1 questo trattamento potrà introdurre nuove modalità e procedure di raccolta dei dati, che non siano sufficientemente trasparenti o siano intrusive?

2.5.2 questo trattamento potrà introdurre modifiche a sistemi e processi, appoggiati a normative in vigore, che possano avere esiti non chiari o non soddisfacenti ?

2.5.3 questo trattamento potrà introdurre modifiche a sistemi e processi, che modifichino il livello di sicurezza dei dati, in modo da portare ad esiti non chiari o non soddisfacenti?

2.5.4 questo trattamento potrà introdurre nuove o modificate procedure sicure di accesso ai dati o modalità di comunicazione e consultazione, che possano essere non chiare o permissive?

2.5.5 questo trattamento introducirà nuove o modificate modalità di conservazione dei dati, che possano essere non chiare o prolungate oltremodo?

2.5.6 questo trattamento modificherà le modalità di messa a disposizione di dati pubblicamente disponibili, in modo tale che i dati diventino più accessibili, in quanto non avveniva in precedenza?

2.6 Esenzioni dalla applicazione delle disposizioni del regolamento - art. 2¹¹

2.6.1 l'attività di trattamento esula dall'ambito delle disposizioni legislative dell'unione europea?

2.6.2 L'attività di trattamento è sviluppata dagli Stati membri, e tali attività non ricadono nell'ambito del capitolo 2 del titolo quinto del trattato dell'unione europea?

2.6.3 Il trattamento è svolto da una persona fisica esclusivamente per fini personali e familiari? In questo caso è anche consentita la diffusione di dati personali che saranno accessibili solo ad un limitato numero di persone, come i familiari e conoscenti?

2.6.4 L'attività di trattamento è svolta da autorità pubbliche al fine di prevenzione, indagine, individuazione e perseguimento di reati o al fine di applicare pene?

2.7 Giustificazioni per l'avvio del progetto di trattamento

2.7.1 le giustificazioni per l'avvio del trattamento includono contributi significativi a misure in grado di migliorare il livello della sicurezza pubblica?

2.7.2 si prevede di sviluppare una consultazione pubblica?

2.7.3 la giustificazione per il nuovo progetto di trattamento dei dati è sufficientemente chiara e sufficientemente pubblicizzata?

Sezione 2 completata da:		Data:	
--------------------------	--	-------	--

¹¹ nota: l'articolo 3 del regolamento prevede alcune esenzioni al campo di applicabilità del regolamento stesso

Sezione 3 - Esito dell'analisi preliminare dei rischi

3.1 Identificazione preliminare dei rischi¹²

La tabella seguente illustra i principali rischi afferenti alla protezione dei dati, che sono stati identificati in fase di valutazione preliminare

	Descrizione del rischio	Valutazione preliminare di esposizione ¹³
Rischio 1		
Rischio 2		
Rischio 3		
Rischio 4		
Rischio 5		
Rischio 6		
Rischio 7		

3.2 Decisione su come procedere¹⁴

Nome di colui che ha assunto la decisione ¹⁵	
Nome di altri soggetti che hanno condiviso questa decisione	

Sezione 3 completata da		Data	
-------------------------	--	------	--

Nota: Se avete deciso che la DPIA non è obbligatoria, ma è comunque sempre raccomandata, andate direttamente alla sezione 6 per portare a termine una più generica valutazione di congruità con le indicazioni del regolamento.

¹² nota: a questo stadio non è ancora opportuno fare una valutazione dettagliata di tutti i rischi, ma prima di procedere con la DPIA è bene aver correttamente identificato i rischi principali

¹³ nota: si raccomanda di fare riferimento la normativa europea EN 31000, che classifica i rischi e i cinque livelli, dal primo livello-accettabile, sino al quinto livello-catastrofico

¹⁴ Nota: dal lavoro sinora sviluppato, siete probabilmente in condizione di stabilire se lo sviluppo di una DPIA è obbligatorio o è solo una valutazione raccomandata. Di seguito spiegate i motivi della conclusione cui siete giunti

¹⁵ nota: ricordate che in data controller è il soggetto che ha la responsabilità finale della decisione

Sezione 4 - Preparazione per la fase di consultazione ed analisi

4.1 Disposizioni afferenti alla Governance¹⁶

Questa DPIA verrà gestita come parte del progetto XXX. Le seguenti persone fisiche, appartenenti al team di progetto, saranno coinvolte nella prosecuzione dello sviluppo del documento

oppure

La DPIA verrà gestita come un progetto separato, cui viene assegnato il nome YYY. Le seguenti persone fisiche faranno parte del team di progetto

oppure

Questa DPIA non è collegata ad un progetto formale e verrà gestita ed approvata da.....

Nome	Ruolo e mansione
	DPIA manager del progetto
	*Aggiungere altri nomi

4.2 Altri soggetti coinvolti, da consultare¹⁷

Soggetto terzo: la nome/organizzazione/ruolo	Quale interesse ha questo soggetto terzo in questo progetto di trattamento ?	Con quali modalità viene sviluppata la consultazione con questo soggetto?

Soggetti interni coinvolti		
Governance aziendale, che viene coinvolta quando i temi legali di congruità sono complessi	Garanzia di congruità con ogni disposizione legislativa applicabile	

4.3 Strategia di consultazione¹⁸

¹⁶ nota: scegliete la risposta più appropriata per completare la tabella. Aggiungere altri nomi e funzioni secondo necessità

¹⁷ nota: questa parte fa riferimento a quanto già sviluppato al punto uno. Tre per identificare i soggetti terzi coinvolti. È appropriato valutare con maggior dettaglio quali sono gli interessi dei vari soggetti terzi coinvolti e il loro coinvolgimento nello sviluppo della DPIA. Non elencare questi soggetti terzi se si fanno già parte del team di progetto o di un team separato coinvolto nell'elaborazione della DPIA

¹⁸ nota: se già viene attuata una strategia di consultazione, afferente a questo progetto, non è necessario elaborarne una separata per lo sviluppo della DPIA. Occorre tuttavia essere certi che questa strategia di consultazione tocchi tutti gli aspetti di protezione dei dati del progetto spiegare in dettaglio che approccio viene adottato al piano di consultazione

4.4 Risorse¹⁹

4.5 consultazione preventiva²⁰

Sezione 4 completata da		Data	
-------------------------	--	------	--

¹⁹ nota: si effettua una valutazione circa la necessità di risorse addizionali, di natura umana od economica, per sviluppare in modo efficace la DPA. Questo caso si verifica con ogni probabilità se l'esito delle consultazioni precedenti sembra aver allargato il campo di applicazione

²⁰ nota: se l'analisi preventiva ha messo in evidenza che le operazioni di trattamento possono presentare un elevato livello di rischio, occorre prendere contatto con l'autorità garante nazionale, secondo quanto indicato all'articolo 36; raccomando di leggerlo attentamente per acquisire informazioni e soddisfare le prescrizioni specifiche

Sezione 5 - Consultazione²¹

5.1 Soggetti terzi coinvolti

Nome del soggetto coinvolto	

5.2 Soggetti interni coinvolti²²

Nome del soggetto coinvolto	Illustrazione di eventuali osservazioni avanzate in fase di consultazione

²¹ nota: per DPIA di grandi dimensioni, laddove molti soggetti sono coinvolti, può esser opportuno sviluppare un rapporto separato circa l'attività di consultazione con i soggetti coinvolti. Le risultanze di questo documento fanno riferimento alla sezione 7. Ricordarsi di completare sempre la sezione 6 per essere certi di svolgere un'attività congrua con il regolamento e altre disposizioni legislative in tema di protezione dei dati.

²² nota: si faccia attenzione a non inserire in questo elenco coloro che fanno parte della squadra che deve elaborare il documento in questione. Come esempio di soggetti interni coinvolti possiamo pensare agli uffici commerciali, vinci marketing, gli uffici amministrativi, che per svolgere la loro attività hanno evidentemente necessità di accedere e trattare dati personali.

Sezione 6 - Congruità con altre leggi, codici o regolamenti afferenti alla protezione dei dati²³

6.1 Indicare il provvedimento

In relazione al provvedimento sopra elencato, è stata effettuata una verifica di conformità, come parte di questa DPIA, secondo quanto illustrato nella appendice A e siamo giunti alla seguente conclusione:

illustrare in dettaglio i motivi della decisione

6.2 Indicare il provvedimento

In relazione al provvedimento sopra elencato, è stata effettuata una verifica di conformità, come parte di questa DPIA, secondo quanto illustrato nella appendice A e siamo giunti alla seguente conclusione:

illustrare in dettaglio i motivi della decisione

6.3 Indicare il provvedimento

In relazione al provvedimento sopra elencato, è stata effettuata una verifica di conformità, come parte di questa DPIA, secondo quanto illustrato nella appendice A e siamo giunti alla seguente conclusione:

illustrare in dettaglio i motivi della decisione

²³ nota: elencare di seguito tutti i provvedimenti legislativi o regolamentari che si applicano alla specifica attività di trattamento ipotizzata; non dimenticare eventuali codici etici od associativi. In particolare, l'articolo 40 del regolamento sulla protezione dei dati fa specifico riferimento a codici di condotta applicabili a specifiche modalità di trattamento. Si raccomanda di leggere attentamente l'articolo 40, punto per punto, onde illustrare il provvedimento e le misure adottate per soddisfare alle indicazioni, sia vincolanti, se indicative, sia orientative, del provvedimento stesso

Sezione 7 - Contenuti analitici della DPIA²⁴

Fare riferimento alla appendice B laddove sono illustrati tutti i rischi identificati e illustrate le opzioni che permettano di mitigare, evitare o mettere sotto controllo questi stessi rischi

7.1 Descrizione analitica delle operazioni di trattamento, con indicazione delle finalità e dei legittimi interessi perseguiti dal DC

7.2 Valutazione della necessità e proporzionalità delle operazioni di trattamento, in relazione alle finalità

7.3 Valutazione dei rischi afferenti ai diritti e alle libertà degli interessati, incluso il rischio di discriminazione connesso o rinforzato dal trattamento

7.4 Descrizione delle misure individuate per mettere sotto controllo i rischi e ridurre al minimo il volume di dati personali da trattare- DPbDefault²⁵

7.5 Elenco dettagliato delle salvaguardie, delle misure di sicurezza e dei meccanismi adottati per garantire la protezione dati personali, come ad esempio la pseudoanonimizzazione, oppure la criptografia, al fine di dimostrare la congruità con il regolamento, tenendo conto dei diritti e dei legittimi interessi degli interessati ed altre persone coinvolte

7.6 Indicazione generale dei limiti di tempo per procedere alla cancellazione delle diverse categorie di dati raccolti

²⁴ nota: l'articolo 35, comma 3, elenca in forma analitica tutte le voci che debbono comporre la DPIA

²⁵ nota: si prenda buona nota anche del fatto che questo tema viene trattato nella DPbD

7.8 Illustrazione di quali procedure di data protection by design e data protection by default verranno adottate, in conformità all'articolo 25

7.9 Elenco dei destinatari o delle categorie di destinatari dei dati personali

7.10 Se applicabile, dare elenco nominativo dei trasferimenti previsti dei dati verso paesi terzi o organizzazioni internazionali²⁶

7.11 Verificare che il trasferimento verso paesi terzi od organizzazioni internazionali rispetti le varie modalità previste, come ad esempio l'inserimento in un elenco di paesi approvati, clausole di salvaguardia, Binding corporate rules o EU-USA privacy shield

7.12 Valutazione del contesto del trattamento dei dati, presso paesi terzi

7.13 Eventuale coinvolgimento del DPO

²⁶ nota: nel caso il trasferimento di dati faccia riferimento all'articolo 46, documentare le appropriate salvaguardie adottate

Sezione 8 - Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati -art 35

8.1 illustrazione del piano di revisione ed aggiornamento del data protection Impact assessment

8.1 Data entro la quale deve essere condotto il riesame di congruità

8.2 Nell'Intervallo di tempo trascorso tra il completamento della prima DPIA e la data entro la quale deve essere condotto il riesame, si sono evidenziate delle modifiche nei rischi connessi al trattamento?²⁷

8.3 Il riesame di congruità ha messo in evidenza delle anomalie?²⁸

8.4 Il riesame di congruità e le eventuali raccomandazioni sono state documentate per iscritto?²⁹

8.5 Se il DC o il DP hanno designato un DPO, quest'ultimo è stato coinvolto nel riesame di congruità?

Sezione completata da:	8	Data:	
---------------------------	---	-------	--

²⁷ nota: in caso di risposta affermativa, illustrare la situazione; in caso di risposta negativa passare al punto 10.4

²⁸ nota: se la risposta è positiva, illustrare le raccomandazioni che permettono di raggiungere un soddisfacente livello di congruità; in caso negativo passare al punto 10.4

²⁹ nota: questo documento deve essere disponibile all'autorità garante nazionale, a richiesta

Sezione 9 - Approvazione della DPIA

9.1 Raccomandazioni³⁰

9.2 Approvazione³¹

Sezione 9 completata da:		Data:	
--------------------------	--	-------	--

³⁰ nota: sulla base della analisi condotta fino a questo punto, indicate quali opzioni siete in grado di raccomandare per procedere. Se rimangono in evidenza rischi significativi, occorre illustrare quale sia il problema e perché fino adesso tale problema non è stato messo sotto controllo. **È possibile che la raccomandazione dell'estensore di questo documento sia di fermare il progetto e riesaminarlo in profondità**

³¹ nota: sottolineare che la approvazione comporta anche la messa disponibile di appropriate risorse umane e materiali; è indispensabile indicare in questa casella chi ha approvato le raccomandazioni del punto 8.1 ed eventuali limitazioni e condizioni che hanno condizionato questa approvazione

Sezione 10 - Attivazione del trattamento ³²

Sezione 10 completata da:		Data:	
------------------------------	--	-------	--

³² nota: illustrare di seguito quali controlli sono stati effettuati prima di avviare l'attività di trattamento, in modo da essere certi che le soluzioni di protezione dei dati approvate come parte di questa valutazione siano efficaci e che il sistema di trattamento sia pienamente conforme alle disposizioni legislative

Appendice A - Lista di controllo della congruità del trattamento previsto con le esigenze di protezione dei dati³³

	Domanda	Risposta
1.	Che tipologie di dati personali devono essere trattate?	
2.	Sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?	
3.	Se vengono trattati speciali categorie di dati, elencati all'articolo 9, paragrafo 1, sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?	
4.	Vi sono aspetti afferenti al rispetto dell'articolo 1, paragrafo 2, del regolamento, che protegge i diritti fondamentali e le libertà delle persone fisiche, ed in particolare il loro diritto alla protezione dei dati personali, che non siano trattati in questa DPIA? ³⁴	
5.	Tutti i dati personali che verranno trattati sono coperti da garanzie di riservatezza? Se sì, come questa riservatezza viene garantita?	
6.	Come viene offerta agli interessati l'informativa in merito al fatto che i loro dati personali verranno raccolti e trattati?	
7.	Il progetto di trattamento dei dati comporta l'utilizzo di dati personali già raccolti, che verranno utilizzati per nuove finalità?	
8.	Quali procedure vengono adottate per verificare che le procedure di raccolta dei	

³³ Nota: Se le risposte a queste domande sono state già date nella sezione 1 di questo documento, fate una riferimento incrociato all'appropriata risposta

³⁴ nota: ricordarsi delle esenzioni previste per le finalità di sicurezza pubblica, indagini penali e simili

	dati sono adeguate, coerenti e non eccessive, in relazione alle finalità per i quali i dati vengono trattati?	
9.	Con quali modalità viene verificata la accuratezza dei dati personali raccolti e trattati?	
10.	È stato effettuato una valutazione circa il fatto che il trattamento dei dati personali raccolti potrebbe causare danno o stress agli interessati coinvolti?	
11.	È stato stabilito un periodo massimo di conservazione dei dati?	
12.	Quali misure tecniche e organizzative di sicurezza sono state adottate per prevenire qualsivoglia trattamento di dati personali non autorizzato o illegittimo?	
13.	È previsto il trasferimento di dati personali in un paese non facente parte dell'unione europea? Se sì, quali provvedimenti sono stati adottati per garantire che i dati siano salvaguardati in modo appropriato?	

Appendice B - Tabella dei rischi afferenti alla DPPIA

³⁵ nota: per ogni rischio afferente alla protezione dei dati, possono essere disponibili varie opzioni che permettono di evitare o mitigare questo rischio. È appropriato elencare tutte le opzioni disponibili e quindi valutare il rischio residuo, in conseguenza dell'applicazione di ogni specifica opzione. Fare riferimento alla normativa europea EN 31000