

DA NECESSITÀ AD OBBLIGO

IL NUOVO REGOLAMENTO PER MOLTI ASPETTI TRASFORMA IN OBBLIGO CIÒ CHE FINO AD ORA ERA “SOLO” UNA NECESSITÀ

Solo qualche esempio, PER GARANTIRE UN ADEGUATO LIVELLO DI TUTELA PER I DATI:

- > PER TRATTAMENTI PIÙ COMPLESSI O DELICATI ERA GIÀ NECESSARIO DOTARSI DI UNA FIGURA DI RIFERIMENTO, POSSIBILMENTE CON COMPETENZE ADEGUATE (**DPO**)
- > AVERE UN “INVENTARIO” DEI TRATTAMENTI È DA SEMPRE NECESSARIO, (SE NON SAI COSA DEVI PROTEGGERE COME FAI A PROTEGGERLO?)
- > **PRIMA DI INIZIARE UNA NUOVA ATTIVITÀ (O TRATTAMENTO) ERA GIÀ NECESSARIO EFFETTUARE UNA SERIE DI VALUTAZIONI CORRELATE ALL’APPLICAZIONE ED AL TRATTAMENTO**
- > UNA ANALISI DEI RISCHI ERA GIÀ NECESSARIA PER GARANTIRE IL RISPETTO DEI PARAMETRI DETTATI DALL’ART. 31 (MISURE DI SICUREZZA “IDONEE”)
- > ISTRUIRE LE FIGURE ATTIVE (CHIUNQUE EFFETTUI UN TRATTAMENTO PER CONTO DEL TITOLARE) È DA SEMPRE NECESSARIO, l’abrogato punto 19 del Disciplinare Tecnico in Allegato B al D. Lgs. 196/2003 definiva un preciso obbligo di formazione.

IL TITOLARE, più di prima, DOVRÀ PENSARE A TUTELARE EFFETTIVAMENTE I DATI ed A DIMOSTRARE DI AVERLO FATTO EFFICACEMENTE

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

NECESSARIO prima di essere obbligatorio

perchè “NECESSARIO”:

“IL TITOLARE DEVE ESSERE IN GRADO DI DIMOSTRARE”

ART. 5 PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («RESPONSABILIZZAZIONE»)

ARTICOLO 24 RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.** Dette misure sono riesaminate e aggiornate qualora necessario.

QUINDI

È NECESSARIO INNANZITUTTO ACQUISIRE **CONSAPEVOLEZZA**

1. INDIVIDUARE COL MAGGIOR DETTAGLIO POSSIBILE:

- > **COSA** (*quali dati tratto*)
- > **PERCHÈ** (*finalità e presupposti di liceità*)
- > **CHI** (*a chi li faccio trattare*)
- > **COME** li tratto (*strumenti utilizzati metodo*)
- > **DOVE** li tratto

È NECESSARIO PROCEDERE CON UNA ATTENTA ANALISI da effettuarsi in relazione ai PIÙ RESTRITTIVI parametri imposti dal Reg. UE 2016/679 che richiedono un maggior dettaglio rispetto a quello comunemente adottato sino ad ora.

2. CLASSIFICARE CORRETTAMENTE I TRATTAMENTI,

**QUESTA FASE È ESSENZIALE PER DEFINIRE NEL MODO PIÙ CORRETTO ED ADERENTE
ALLE ESIGENZE (aziendali e di tutela dei dati)
I PERIMETRI DI INTERVENTO E LE AREE DA AFFRONTARE UNITARIAMENTE**

SI SUGGERISCE DI PROCEDERE PER PROCESSO O FAMIGLIE DI PROCESSI
prendendo quale riferimento quale fattore accomunante l'elemento che più incide sulla
corretta gestione della tutela dei dati presente in ogni processo/Attività,
scegliendo, ad esempio, tra:

- > **tipologia di RAPPORTO CON GLI INTERESSATI** (particolarmente impattante sulle modalità di gestione degli obblighi di informativa e consenso)
- > **FINALITÀ**
- > **SISTEMI o PARTICOLARI TECNOLOGIE** (che possono presentare rischi aggiuntivi, ES.: GPS, Videosorveglianza)
- > **PARTICOLARE NATURA DEI DATI e/o altri trattamento o contesti su cui il Garante si sia già pronunciato con provvedimenti a carattere generale**

**IL LIVELLO DI DETTAGLIO NELLA CLASSIFICAZIONE DEI TRATTAMENTI DIPENDE ANCHE
DALLA VOSTRA STRUTTURA ORGANIZZATIVA**

es.:

una eccessiva frammentazione calata su una organizzazione molto snella può complicare la gestione

in una struttura più articolata sarà necessario utilizzare come riferimento anche aspetti organizzativi in modo da correlare più facilmente il trattamento alla/e unità operativa/e coinvolte

**NON ESISTE UN SISTEMA MIGLIORE IN ASSOLUTO
ESISTE IL SISTEMA MIGLIORE PER IL VOSTRO CONTESTO**

“REGISTRO DEI TRATTAMENTI” Cosa dice il GARANTE

*Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.*

RACCOMANDAZIONI

*La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.*

*Nello specifico, si richiama l'attenzione sulla sostanziale **coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice (*) e quelli che devono costituire il registro dei trattamenti ex art. 30 regolamento**; l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni.*

() La notificazione è validamente effettuata solo se è trasmessa attraverso il sito del Garante, utilizzando l'apposito modello, che contiene la richiesta di fornire tutte e soltanto le seguenti informazioni:*

- a) le coordinate identificative del titolare del trattamento e, eventualmente, del suo rappresentante, nonché le modalità per individuare il responsabile del trattamento se designato;*
- b) la o le finalità del trattamento;*
- c) una descrizione della o delle categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime;*
- d) i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;*
- e) i trasferimenti di dati previsti verso Paesi terzi;*
- f) una descrizione generale che permetta di valutare in via preliminare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento*

La classificazione proposta è coerente con il titolo dell'art. 30 che rimarca il concetto di ATTIVITÀ DI TRATTAMENTO (insieme di trattamenti)

ARTICOLO 30 - REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

1. **Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.** Tale registro contiene tutte le seguenti informazioni:
 - a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
 - b) le finalità del trattamento;
 - c) una descrizione delle categorie di interessati e delle categorie di dati personali;
 - d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
 - e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
 - f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
 - g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. **Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:**
 - a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
 - b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
 - c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
 - d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. **I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.**
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
5. *Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale*

o

include il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

IL REGISTRO È OBBLIGATORIO per

1. IMPRESE CON PIÙ DI 250 “*DIPENDENTI*”
2. IMPRESE CHE EFFETTUANO TRATTAMENTI CHE POSSA PRESENTARE UN RISCHIO PER I DIRITTI E LE LIBERTÀ DELL'INTERESSATO IN MODO NON OCCASIONALE
3. TITOLARI e RESPONSABILI che trattino categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

1. IMPRESE CON PIÙ DI 250 “*DIPENDENTI*”

MA: “meno di 250 dipendenti” è la traduzione di “employing fewer than 250 persons” . . .

2. IMPRESE CHE EFFETTUANO TRATTAMENTI CHE POSSANO PRESENTARE UN RISCHIO PER I DIRITTI E LE LIBERTÀ DELL'INTERESSATO IN MODO NON OCCASIONALE

OCCASIONALE: “*Che dipende da un’occasione, che nasce dalle particolari circostanze, e quindi non voluto o cercato appositamente, casuale, fortuito.
Temporaneo*”

Per una prima identificazione di trattamenti che possono *presentare un rischio per i diritti e le libertà dell'interessato* ci vengono in aiuto:

- > l'art. 37 D. Lgs. 196/2003 (*Se ho dovuto notificare un trattamento dovrò redigere il registro e, probabilmente, effettuare una VIP*)
- > e l'art. 35 del Reg. UE 2016/679 (*il Titolare che deve procedere con una VIP deve redigere il registro obbligatoriamente*)

- Art. 37 D. Lgs. 196/2003 c.1 (NOTIFICAZIONE)

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

- a) dati **genetici, biometrici** o dati che indicano la **posizione geografica** di persone od oggetti mediante una rete di comunicazione elettronica;
- b) dati idonei a rivelare lo **stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;**
- c) dati idonei a rivelare la **vita sessuale o la sfera psichica** trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- d) dati **trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato,** o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- e) **dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;**
- f) **dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.**

art. 35 del Reg. UE 2016/679

- “(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;
- (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; o
- (c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico”

Nelle “Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento “possa presentare un rischio elevato” ai sensi del regolamento 2016/679” (disponibili sul sito del Garante) sono forniti alcuni ESEMPI:

UN TITOLARE PUÒ RITENERE, NELLA MAGGIORANZA DEI CASI, CHE QUANDO UN TRATTAMENTO SODDISFA **DUE DEI CRITERI DI SEGUITO INDICATI SIA NECESSARIO CONDURRE UNA DPIA (VIP).**

- 1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive,** in particolare a partire da “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).

A titolo esemplificativo si possono citare un istituto finanziario che effettui lo screening dei propri clienti utilizzando un database di rischio creditizio ovvero un database per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF); una società operante nel settore delle biotecnologie che offra test genetici direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; una **società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web**.

- 2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga**

natura: trattamenti finalizzati ad assumere decisioni su interessati che producano “effetti giuridici sulla persona fisica” ovvero che “incidono in modo analogo significativamente su dette persone fisiche” (art. 35, paragrafo 3, lettera a)). Per esempio, il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione. Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio. Per maggiori dettagli sui concetti in gioco si rimanda alle Linee-guida in materia di profilazione che il Gruppo di lavoro si appresta a pubblicare.

- 3. Monitoraggio sistematico:** trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o “la sorveglianza sistematica di un'area accessibile al pubblico” (art. 35, paragrafo 3, lettera c)). Questa tipologia di monitoraggio costituisce un criterio, ai fini della DPIA, in quanto la raccolta di dati personali può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo e per quali finalità. Inoltre, è talora impossibile per gli interessati sottrarsi a questa tipologia di trattamenti in aree pubbliche (o pubblicamente accessibili).

- 4. Dati sensibili o dati di natura estremamente personale:** si tratta delle categorie particolari di dati personali di cui all'art. 9 (per esempio, informazioni sulle opinioni politiche di una persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10.

A titolo di esempio, si può citare un ospedale che conserva le cartelle cliniche dei pazienti, o un investigatore privato che conserva informazioni su soggetti responsabili di reati. Al di là di queste disposizioni del regolamento, vi sono talune categorie di dati che possono aumentare i rischi eventuali per i diritti e le libertà delle persone fisiche. Si tratta di dati personali considerati sensibili (nell'accezione comune del termine), in quanto connessi alla vita familiare o privata (quali i **dati relativi alle comunicazioni elettroniche** dei quali occorre tutelare la riservatezza) ovvero in quanto incidono sull'esercizio di un diritto fondamentale (quali i **dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione**) ovvero in quanto una loro violazione comporta evidentemente un grave impatto sulla vita quotidiana dell'interessato (quali i **dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti**). A tale proposito, può essere pertinente la circostanza per cui i dati siano già stati resi pubblici dall'interessato ovvero da terzi. Il fatto che un certo dato personale sia disponibile pubblicamente può essere un elemento da prendere in esame nel valutare l'aspettativa di un utilizzo ulteriore di tale dato per determinati scopi. Il criterio in oggetto può riferirsi anche a dati quali documenti personali, email, agende, appunti tratti da lettori elettronici dotati di dispositivi per la presa di appunti, e **informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita**.

- 5. Trattamenti di dati su larga scala:** il regolamento non offre definizioni del concetto di “larga scala”, anche se il considerando 91 fornisce indicazioni in merito. In ogni caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala:

- numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;
- volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;
- durata, o persistenza, dell'attività di trattamento;

d. ambito geografico dell'attività di trattamento.

6. Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato.

7. Dati relativi a interessati vulnerabili (considerando 75): il trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che **il singolo può non disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti.**

La categoria degli interessati vulnerabili **comprende anche i minori**, che si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali, **i dipendenti**, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (**soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti**) e ogni interessato per il quale si possa identificare una situazione di **disequilibrio** nel rapporto con il rispettivo titolare del trattamento.

8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative, come **l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici**, e così via. Il regolamento chiarisce (art. 35, paragrafo 1, e considerando 89 e 91) che l'utilizzo di una nuova tecnologia, definito "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare l'obbligo di condurre una DPIA, in quanto il ricorso a una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone. Nei fatti, le conseguenze sul piano individuale e sociale del ricorso a una nuova tecnologia sono talora ignote. La DPIA aiuterà il titolare a comprendere e gestire tali rischi. Per esempio, alcune applicazioni legate all' "Internet delle cose" potrebbero avere impatti significativi sulla vita privata e le abitudini delle persone, e, quindi, necessitano di una DPIA.

9. Tutti quei trattamenti che, di per sé, "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto" (art. 22 e considerando 91). Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto. Si pensi, a titolo di esempio, allo **screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.**

3.

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI DI CUI ALL'ARTICOLO 9, PARAGRAFO 1, O I DATI PERSONALI RELATIVI A CONDANNE PENALI E A REATI DI CUI ALL'ARTICOLO 10.

c.1 art. 9: **DATI “PARTICOLARI”**: <<... dati personali che rivelino

l'origine razziale o etnica,

le opinioni politiche,

le convinzioni religiose o filosofiche, o

l'appartenenza sindacale,

dati genetici,

dati biometrici intesi a identificare in modo univoco una persona fisica,

dati relativi alla salute o

alla vita sessuale o all'orientamento sessuale >>

13) «**DATI GENETICI**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, **e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione**;

14) «**DATI BIOMETRICI**»: i dati personali ottenuti da un trattamento tecnico **specifico** relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica **che ne consentono o confermano l'identificazione univoca**, quali **l'immagine facciale** o i dati **dattiloscopici**;

[CONSIDERANDO (51).....Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica.]

15) «**DATI RELATIVI ALLA SALUTE**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

CONTENUTI PREVISTI PER IL TITOLARE

art. 30 Reg UE 2016/679	
a) il nome e i dati di contatto del titolare del trattamento	contenuto ovviamente comune a tutti i trattamenti elencati nel registro
e, ove applicabile, del contitolare del trattamento,;	Contenuto che può essere riferito anche ad un solo trattamento
del rappresentante del titolare del trattamento e	contenuto ovviamente comune a tutti i trattamenti elencati nel registro
del responsabile della protezione dei dati	contenuto ovviamente comune a tutti i trattamenti elencati nel registro se nominato
b) le finalità del trattamento;	contenuti rintracciabili sulle informative ex art. 13 D. Lgs.196/2003 già redatte
c) una descrizione delle categorie di interessati;	
e delle categorie di dati personali	
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;	
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e	necessario effettuare verifiche
, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;	
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;	importante: costituisce peraltro uno dei nuovi contenuti della informativa
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1	Adottando un approccio minimale, non sempre sufficiente, potrebbero essere prese a riferimento le semplici tabelle proposte dal Garante per la compilazione del DPS. Chi ha redatto e continuato ad aggiornare efficacemente il D.P.S. non avrà difficoltà. N.B. distinguere tra le misure di sicurezza "perimetrali" (che riguardano tutti i trattamenti) e quelle applicate sul singolo trattamento.

**MINORI CONTENUTI PREVISTI PER IL REGISTRO COMPILATO IN QUALITÀ DI
“RESPONSABILE” ex art. 28 Reg. UE 679****art. 30 Reg UE 2016/679**

- | |
|--|
| a) il nome e i dati di contatto del RESPONSABILE O DEI RESPONSABILI del trattamento
di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento
del rappresentante del titolare del trattamento e
del responsabile della protezione dei dati |
| b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; |
| C) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e
, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; |
| g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 |

**I CONTENUTI SOPRA INDICATI NON SONO SUFFICIENTI PER MONITORARE
CORRETTAMENTE TUTTI I SERVIZI POTENZIALMENTE EROGATI DA UN RESPONSABILE
UTILE AGGIUNGERE UNA DESCRIZIONE DEL TRATTAMENTO E DELLE OPERAZIONI
DELEGATE DAL TITOLARE AL RESPONSABILE**

Articolo 32 Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
 - a) la pseudonimizzazione e la cifratura dei dati personali;
 - b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO
svolte in qualità di TITOLARE
eempio indicativo

evidenziati in giallo i contenuti obbligatori

INDICE

DATI GENERALI

ELENCO TRATTAMENTI CENSITI - QUADRO SINOTTICO (SUGGERITO)

SCHEDE DESCRITTIVE ATTIVITÀ DI TRATTAMENTO

DESCRIZIONE MISURE DI SICUREZZA

- > **TECNICHE**
- > **ORGANIZZATIVE**
- > **FISICHE**

MODALITÀ CLASSIFICAZIONE ATTIVITÀ DI TRATTAMENTO (MACROTRATTAMENTO)

È stato adottato un sistema di classificazione dei trattamenti basato sull'articolazione delle attività e processi, correlati in base alla loro natura, in modo da rispecchiarne quanto più possibile l'organizzazione.

In questo modo le operazioni/trattamenti (*che in base alla definizione normativa sono considerabili trattamenti anche se prese a se stanti*) che presentano caratteristiche omogenee ai fini della tutela della privacy e dell'applicazione della normativa, vengono raggruppate sotto un'unica voce definita in modo da identificare la caratteristica che le accomuna e che può essere distintiva, ad esempio, della finalità principale, di una categoria di interessati, di specifiche modalità di gestione, della tecnologia utilizzata o della tipologia di dati personali.

DATI GENERALI [obbligatorie]**Titolare**

Nome e cognome o denominazione o ragione sociale

Stato

Via/piazza

N. civ.

Comune

C.a.p.

Prov.

Telefono

Fax

E-mail

Legale rappresentante

E' stato nominato un Responsabile Protezione Dati?

Il Titolare e' stabilito fuori dell'Unione Europea e si deve pertanto designare un rappresentante in Italia?

RESPONSABILE PROTEZIONE DATI**Indirizzo e contatti** (se diversi da quelli del Titolare)

Via/Piazza

N. civ.

Localita'

C.a.p.

Prov.

Tel.

Fax

E-mail

Rappresentante del titolare stabilito nel territorio di un paese non appartenente all'UE

Nome e cognome o denominazione o ragione sociale

Indirizzo

Via/Piazza

N. civ.

Localita'

C.a.p.

Prov.

Tel.

Fax

E-mail

ELENCO TRATTAMENTI CENSITI - QUADRO SINOTTICO**NOTE:**

(#) _____ indicare se l'attività comprende dati Sensibili/Particolari, Giudiziari, relativi alla Salute, Biometrici, Genetici, dati di geolocalizzazione o altri dati che ancorché non sensibile/particolare o giudiziario, debbano essere gestiti con particolare prudenza poiché il loro trattamento genera un rischio per l'interessato specificando anche se la presenza di tali dati sia "non sistematica-occasionale/incidentale"

(0) rif....._effettuata VIP

(1) _____ Trattamento trattamento effettuato in regime di contitolarità

(2) _____ Trattamento affidato, anche solo in parte a soggetti esterni

(3) rif....._ Trattamento effettuato per conto di soggetti esterni, in alcuni casi in qualità di Responsabile ex art. 29 D. Lgs. 196/2003 indicare voce di riferimento su registro dei trattamenti compilato in qualità di responsabile EX ART. 28 reg. UE 679

COD.	TRATTAMENTO	categorie interessati	DATI (#)	Finalità principale - particolari modalità	rif. scheda n° Funzione di riferimento primaria u.o. di riferimento NOTE
	Amministrazione personale - PAYROLL	Personale dipendente e non dipendente parificato - familiari o conviventi dei dipendenti		amministrazione del personale ed adempimento relativi obblighi. elaborazione buste paga ed attività correlate	1 RISORSE UMANE (2)
	PREVENZIONE E PROTEZIONE	Lavoratori (dipendenti ed esterni)		Gestione SPP Adempimenti T.U.S. Sorveglianza sanitaria	2 RSPP (2)
	geolocalizzazione	Clienti-Utenti Management, personale incaricato da clienti Utenti Privati		erogazione servizi correlati alla elaborazione - messa a disposizione e conservazione di dati di geolocalizzazione per conto del cliente.	3 SERVIZIO ICT (0) RIF. VIP N.1 (2) (3)
	GESTIONE SISTEMI ICT	Utenti sistemi informatici aziendali - <i>interessati con cui hanno rapporti il titolare e gli utenti dei sistemi</i>		Gestione Sistemi Informatici e telefonici Aziendali – Sicurezza assegnazione strumenti e devices mobili	4 SERVIZIO ICT (0) RIF. VIP N.1 (2) (3)

SCHEDA ATTIVITÀ DI TRATTAMENTO N°

ATTIVITÀ DI TRATTAMENTO

COD.

COMPILATA VALUTAZIONE DI IMPATTO

NO

SI

RIF.

L'attività di trattamento è svolta in regime di contitolarità?

☐

SI

☐

NO

CONTITOLARE/I
[obbligatorio]

Nome e Cognome o denominazione o ragione sociale, indirizzo, telefono, fax, e-mail

il contitolare ha nominato UN RESPONSABILE PROTEZIONE DATI?

☐

SI

☐

NO

Nome e dati di contatto

OPERAZIONI DI COMPETENZA DEL CONTITOLARE

DESCRIZIONE DELLE CATEGORIE DI INTERESSATI E DELLE CATEGORIE DI DATI PERSONALI

*Una attività di trattamento può coinvolgere più di una categorie di interessati e non prevede le stesse categorie di dati personali per tutti gli interessati coinvolti
(questa correlazione non è prevista dalla Notificazione)*

DESCRIZIONE DELLE CATEGORIE DI INTERESSATI E DELLE CATEGORIE DI DATI PERSONALI

CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	DESCRIZIONE fonte acquisizione/origine - addetti	TERMINE ULTIMO PREVISTI PER LA CANCELLAZIONE o CRITERI adottati [obbligatorio]
CLASS INTERESSATI "LARGA SCALA" ☐ SI ☐ NO	P= Categorie "Particolari" (ex "sensibili") ☐ dati che rivelano l'origine razziale o etnica ☐ dati che rivelano le opinioni politiche		
	☐ dati che rivelano le convinzioni religiose o filosofiche		
	☐ dati che rivelano l'appartenenza sindacale		
	☐ dati relativi alla vita/orientamento sessuale		
	☐ S = relativi alla Salute		
	☐ B = Biometrici		
	☐ GG = Genetici		
	G = Giudiziari R = Speciali o "estremamente personali" ALTRI		
CLASS INTERESSATI			
CLASS INTERESSATI			

FINALITÀ [obbligatorio]	fondamento di LICEITÀ RIF REG.UE 2016/679 ART.6
una "attività di trattamento" può rispondere a più finalità	

DESCRIZIONE DEL TRATTAMENTO	
CONTENUTO PREVISTO DALLA NOTIFICAZIONE MA NON DALL'ART. 30 REG.UE 679	
MOLTI INDICANO LE OPERAZIONI DESCRITTE NELLA DEFINIZIONE DI "TRATTAMENTO" MOLTI PROCEDONO CON UNA DESCRIZIONE DEL TRATTAMENTO CHE PRENDE LE MOSSE DALLA DEFINIZIONE che, però, fornisce solo degli esempi costituisce, quindi un APPROCCIO LIMITATO E POTENZIALMENTE FUORVIANTE, tuttavia vi sono alcune categorie di operazioni che è opportuno tracciare adeguatamente (evidenziate in azzurro):	
	VOCI CONTENUTE NELLA DEFINIZIONE ART. 4 REG. UE 2016/679
	RACCOLTA - REGISTRAZIONE
	interconnessione
	CONSERVAZIONE
	CONSULTAZIONE
	MODIFICA
	organizzazione
	strutturazione elaborazione
	adattamento selezione
	estrazione
	raffronto
	CANCELLAZIONE - DISTRUZIONE
	COMUNICAZIONE mediante trasmissione
	qualsiasi altra forma di messa a disposizione
	DIFFUSIONE
	LIMITAZIONE (ex blocco)
	USO
	ALTRE VOCI
	ARCHIVIAZIONE
	RIPRODUZIONE - COPIA
	4) « PROFILAZIONE »: 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 ;
	5) « PSEUDONIMIZZAZIONE »: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile ;
	3) « LIMITAZIONE DI TRATTAMENTO »: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
	[considerando (67) Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.]

VALUTAZIONE PIA

Un titolare può ritenere, nella maggioranza dei casi, che quando un trattamento soddisfa **due dei criteri sotto indicati sia necessario condurre una DPIA**

1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, in particolare a partire da <i>“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”</i> .	
2. Decisioni <u>automatizzate</u> che producono significativi effetti giuridici o di analoga natura: trattamenti finalizzati ad assumere decisioni su interessati che producano <i>“effetti giuridici sulla persona fisica”</i> ovvero che <i>“incidono in modo analogo significativamente su dette persone fisiche”</i> (art. 35, paragrafo 3, lettera a)	
3. Monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o <i>“la sorveglianza sistematica di un'area accessibile al pubblico”</i> (art. 35, paragrafo 3, lettera c)	
4. Dati sensibili o dati di natura estremamente personale: si tratta delle categorie particolari di dati personali di cui all'art. 9 (per esempio, informazioni sulle opinioni politiche di una persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10.	
5. Trattamenti di dati su larga scala: il regolamento non offre definizioni del concetto di “larga scala”, anche se il considerando 91 fornisce indicazioni in merito. In ogni caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala: a. numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; b. volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; c. durata, o persistenza, dell'attività di trattamento; d. ambito geografico dell'attività di trattamento.	
6. Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti,	
7. Dati relativi a interessati vulnerabili (ES. minori, dipendenti, ETC) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.	
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative,	
9. Tutti quei trattamenti che, di per sé, <i>“impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto”</i> .	

PREVISTA LA DIFFUSIONE NO ☐ SI ☐ DESCRIZ.

CATEGORIE DI DESTINATARI A CUI I DATI PERSONALI SONO STATI O SARANNO COMUNICATI, COMPRESI I DESTINATARI DI PAESI TERZI OD ORGANIZZAZIONI INTERNAZIONALI [obbligatorio]

CATEGORIE DI DESTINATARI o DESTINATARIO
[obbligatorio]

ORGANIZZAZIONE INTERNAZIONALE O SITO PAESE TERZO
[obbligatorio]

documentazione delle garanzie adeguate per trasferimenti di cui al secondo comma dell'articolo 49 (*)
[obbligatorio]

(*) per l'art. 49, comma 2, "...che sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, **non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro**. Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari

DESCRIZIONE MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE RIFERITE AL TRATTAMENTO

[obbligatorio]

ALTRI CONTENUTI SUGGERITI/NECESSARI:

FUNZIONE DI RIFERIMENTO PRIMARIA

ALTRE STRUTTURE CHE CONCORRONO AL TRATTAMENTO

TRATTAMENTO DELEGATO, ANCHE SOLO IN PARTE, A RESPONSABILI NO ☐ SI ☐

RESPONSABILE	NATURA DEL SERVIZIO EROGATO O DESCRIZIONE DEL TRATTAMENTO	CONTATTI	REFERENTE E/O DPO	NOTE

STRUMENTI ICT IMPIEGATI

ALTRI STRUMENTI

INDICAZIONE ARCHIVI FISICI

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE ADOTTATE

[obbligatorio]

tabelle per approccio minimo desunte dalla "Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS) pubblicata dall'Autorità Garante "

Tenuto conto degli obblighi di cui all'art. 32 del Reg. UE679 e di quanto riportato all'art. 24 (.....,il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. ...) il Titolare deve dotarsi di adeguate misure di sicurezza possibilmente descritte in separati documenti, che potrebbero essere qui richiamate anche solo con un richiamo alla procedura di riferimento.

Misure	Rischi contrastati	Trattamenti interessati	RIF. SCHEDA o procedura aziendale	Struttura o persone addette all'adozione

SCHEDA DESCRITTIVA DELLE MISURE ADOTTATE

Scheda nr.		Compilata da		Data di compilazione	
Misura					
Descrizione sintetica					
Data aggiornamento:					

CRITERI E PROCEDURE PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Data base/archivio	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino

CRITERI E PROCEDURE PER IL SALVATAGGIO DEI DATI

Sistema	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti

CRITERI E PROCEDURE PER valutare regolarmente l'efficacia delle misure tecniche e organizzative

Descrizione	Pianificazione

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO
svolte in qualità di RESPONSABILE
esempio indicativo

*evidenziati in **giallo** i contenuti obbligatori*

INDICE

DATI GENERALI

ELENCO TRATTAMENTI svolti in qualità di Responsabile - QUADRO SINOTTICO

SCHEDE DESCRITTIVE ATTIVITÀ DI TRATTAMENTO

DESCRIZIONE MISURE DI SICUREZZA

MODALITÀ CLASSIFICAZIONE ATTIVITÀ DI TRATTAMENTO (MACROTRATTAMENTO)

**per questo contenuto potrebbe essere necessario coordinarsi nel metodo con il TITOLARE O
IL RESPONSABILE PER CONTO DEL QUALE VIENE EFFETTUATO CIASCUN TRATTAMENTO**

DATI GENERALI^[obbligatori]

RESPONSABILE COMPILATORE

Nome e cognome o denominazione o ragione sociale			
Stato			
Via/piazza			
N. civ.			
Comune			
C.a.p.		Prov.	
Telefono		Fax	
E-mail			
Legale rappresentante			

SOGGETTO CHE HA NOMINATO IL COMPILATORE IN QUALITÀ DI☐ **TITOLARE DEL TRATTAMENTO**☐ **RESPONSABILE AUTORIZZATO DAL TITOLARE DEL TRATTAMENTO**

N.B.: CONTENUTO OBBLIGATORIO - PER TRATTAMENTI SVOLTI IN MODO RIPETITIVO E CONNESSI ALLA EROGAZIONE DI UN SERVIZIO L'INDICAZIONE DEI TITOLARI POTREBBE ESSERE COSTITUITA DA UN COLLEGAMENTO A SCHEDE O BANCHE DATI ANAGREFICHE DEI CLIENTI (TITOLARI DEL TRATTAMENTO) CON INDICAZIONE DEI PRODOTTI/SERVIZI ACQUISTATI

Nome e cognome o denominazione o ragione sociale	
Stato	
Via/piazza	
N. civ.	
Comune	
C.a.p.	
Prov.	
Telefono	
Fax	
E-mail	
Legale rappresentante	

RESPONSABILE PROTEZIONE DATI

Indirizzo e contatti (se diversi da quelli del Titolare)

Via/Piazza		
N. civ.		
Località		
C.a.p.		Prov.
Tel.		Fax
E-mail		

Rappresentante del titolare stabilito nel territorio di un paese non appartenente all'UE

Nome e cognome o denominazione o ragione sociale

Indirizzo

Via/Piazza		
N. civ.		
Località		
C.a.p.		Prov.
Tel.		Fax
E-mail		

ELENCO TRATTAMENTI - QUADRO SINOTTICO**NOTE:**

- (#) _____ indicare se l'attività comprende dati Sensibili/Particolari, Giudiziari, relativi alla Salute, Biometrici, Genetici, dati di geolocalizzazione o altri dati che ancorché non sensibile/particolare o giudiziario, debbano essere gestiti con particolare prudenza poiché il loro trattamento genera un rischio per l'interessato specificando anche se la presenza di tali dati sia "non sistematica-occasionale/incidentale"
- (0) rif..... coadiuvato il titolare nel compilare una VIP
- (2) _____ Trattamento affidato, anche solo in parte, ad Aziende collegate o a soggetti esterni
- (4) _____ Comprende trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale

COD .	TRATTAMENTO	categorie interessati	categorie DATI (#)	DESCRIZIONE	rif. scheda n° NOTE
	AMMINISTRAZIONE DEL PERSONALE	Personale dipendente e non dipendente parificato - familiari o conviventi dei dipendenti DEL TITOLARE			
	geolocalizzazione	Clients-Utenti Management, personale incaricato da clienti			
	GESTIONE SISTEMI ICT	Utenti sistemi informatici gestiti per conto del titolare			

SCHEDA ATTIVITÀ DI TRATTAMENTO N°

ATTIVITÀ DI TRATTAMENTO

COD.

TITOLARE/I
[obbligatorio]

Nome e Cognome o denominazione o ragione sociale, indirizzo, telefono, fax, e-mail

DESCRIZIONE DELLE CATEGORIE DI INTERESSATI E DELLE CATEGORIE DI DATI PERSONALI
(ove possibile)

CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	DESCRIZIONE	
TIPO INTERESSATO	Sensibili/Particolari		
	• dati (O DOCUMENTI) che rivelano l'origine razziale o etnica		
	• dati che rivelano le opinioni politiche		
	• dati che rivelano le convinzioni religiose o filosofiche		
	• dati che rivelano l'appartenenza sindacale		
	• dati relativi alla vita/orientamento sessuale		
	S = relativi alla Salute		
	B = Biometrici		
	GG = Genetici		
	G = Giudiziari		
	Ge = geolocalizzazione		
	R = Speciali		
	altri		

DESCRIZIONE DEL TRATTAMENTOPREVISTA LA DIFFUSIONE NO ☐ SI ☐ DESCRIZ.**CATEGORIE DI DESTINATARI A CUI I DATI PERSONALI SONO COMUNICATI, COMPRESI I DESTINATARI DI PAESI TERZI OD ORGANIZZAZIONI INTERNAZIONALI** [obbligatori]

CATEGORIE DI DESTINATARI o DESTINATARIO	ORGANIZZAZIONE INTERNAZIONALE O SITO PAESE TERZO	documentazione delle garanzie adeguate per trasferimenti di cui al secondo comma dell'articolo 49

DESCRIZIONE MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE RIFERITE AL SINGOLO TRATTAMENTO
[obbligatorio]**ALTRI CONTENUTI SUGGERITI/NECESSARI:****ALTRE STRUTTURE CHE CONCORRONO AL TRATTAMENTO**

STRUMENTI ICT IMPIEGATI

ALTRI STRUMENTI

INDICAZIONE ARCHIVI FISICI

TRATTAMENTO DELEGATO, ANCHE SOLO IN PARTE, A RESPONSABILI NO ☐ SI ☐

RESPONSABILE	NATURA DEL SERVIZIO EROGATO	CONTATTI	REFERENTE	NOTE

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE ADOTTATE [obbligatorio]
tabelle per approccio minimo desunte dalla “Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS) pubblicata dall’Autorità Garante “

questi contenuti coincidono con quelli del registro compilato in qualità di Titolare

Tenuto conto degli obblighi di cui all’art. 32 del Reg. UE679 il Responsabile deve dotarsi, se del caso in accordo con il titolare, di adeguate misure di sicurezza possibilmente descritte in separati documenti, che potrebbero essere qui richiamate anche solo con un richiamo alla procedura di riferimento. Analogo approccio per le ulteriori misure/procedure imposte eventualmente dal Titolare

Misure	Rischi contrastati	Trattamenti interessati	RIF. SCHEDA o procedura aziendale	Struttura o persone addette all’adozione

SCHEDA DESCRITTIVA DELLE MISURE ADOTTATE

Scheda nr.		Compilata da		Data di compilazione	
Misura					
Descrizione sintetica					
Data aggiornamento:					

CRITERI E PROCEDURE PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Data base/archivio	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino

CRITERI E PROCEDURE PER IL SALVATAGGIO DEI DATI

Sistema	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti

CRITERI E PROCEDURE PER valutare regolarmente l'efficacia delle misure tecniche e organizzative

Descrizione	Pianificazione