1. DEFINIZIONI E ACRONIMI

1.1 Definizioni

Termine	Descrizione
Trattamento	Ex art. 4, numero 2 del GDPR: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"
Titolare del trattamento	Ex art. 4, comma 7 del GDPR: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri"
Responsabile del trattamento	Ex art. 4, comma 8 del GDPR: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"
Anonimizzazione	Tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.
Accountability	Ex art. 5, paragrafo 2 del GDPR: "Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)". Il paragrafo 1 dell'art. 5 del GDPR riguarda i principi fondamentali che devono essere accuratamente applicati ai trattamenti di dati personali
Dati biometrici	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.
Dati relativi alla salute	Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria,

Termine	Descrizione
	che rivelano informazioni relative al suo stato di salute.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Interessato	Persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Misure di sicurezza	Misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.

1.2 Acronimi

Termine	Descrizione
GDPR	General Data Protection Regulation
DT	Delegato del Titolare
RPD / DPO	Responsabile della Protezione dei Dati Personali / Data Protection Officer

2.REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

"Si tratta di qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".
[Articolo 4 EU RGPD]

2.1 Ambito di applicazione

Al fine di uniformarsi al Regolamento Europeo nr. 679/2016 (General Data Protection Regulation meglio noto come GDPR), entrato in vigore il 24 maggio 2016 e applicabile a partire dal 25 maggio 2018, è necessario porre attenzione al processo di istituzione e conservazione del registro di trattamenti in capo ai titolari e responsabili del trattamento con l'obiettivo di avere una chiara panoramica dei trattamenti di dati personali che fanno capo appunto al titolare secondo il principio fondamentale dell'accountability.
La normativa introduce a fianco dei Titolari e dei Responsabili dei trattamenti, obbligatoriamente per gli enti pubblici, la figura Data Protection Officer – DPO, che funge da consulente per le figure di cui sopra verificando la compliance dell'Ente rispetto al regolamento ma anche come referente dell'Ente per i soggetti interessati che necessitano di un riferimento in materia di protezione dei dati personali.
La responsabilità della tenuta del registro è del titolare o suo delegato, l'utilità di ciò è l'identificazione dei trattamenti e la conseguente analisi del rischio di ciascuno. Il registro può essere tenuto in forma scritta o elettronica e deve essere esibito nel caso di richiesta esplicita da parte delle autorità di controllo.

2.2.La normativa

In ottemperanza alla normativa, nello specifico all'art 30 del GDPR, in relazione al Registro delle attività di trattamento si riportano i dettami della norma:

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 includa 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.

Per ulteriori precisazioni si faccia riferimento al considerando 82 del Regolamento.

2.3 Struttura del registro

Il registro è costituito da una prima sezione l'**Intestazione,** che contiene i seguenti dati che vanno compilati e aggiornati ad ogni modifica effettuata sul registro:

- **Titolare del trattamento** (Denominazione, Indirizzo, n telefono, mail,PEC);
- **Delegato del titolare** (Denominazione, Indirizzo, n telefono, mail,PEC);
- **Responsabile protezione dei dati(DPO) ***(Nome e Cognome o ragione sociale, Indirizzo, n telefono, mail,PEC); (*) se non nominato è consigliabile scrivere in questo campo le motivazioni della mancata nomina
- **Altre info da aggiornare ad ogni modifica:** (Registro tenuto da, data creazione, ultimo aggiornamento, n. schede compilate,prossima revisione).

Il registro è un documento interno e va esibito alle autorità di controllo (Garante) in caso di verifiche, deve essere pertanto costantemente aggiornato e deve recare "in maniera verificabile" sia la data della sua prima istituzione o creazione sia la data dell'ultimo aggiornamento.

Gli enti del settore pubblico sono tenuti a comunicare il registro a chiunque lo richieda, trattandosi di un documento amministrativo, ovviamente previo oscuramento delle informazioni vietate ai sensi di legge e che potrebbero nuocere a terzi. Trattandosi di documento interno, per gli altri settori che non sia appunto il publico, non si è tenuti a comunicarlo o condividerlo con nessuno, eccetto ovviamente le autorità in caso di verifica.

Il principio cardine del GDPR dell'accountability , ovvero la responsabilizzazione del titolare di un trattamento dati, sancisce che ad essere responsabile delle proprie scelte in merito a finalità e modalità del trattamento che pone in essere nel sistema normativo delineato dal GDPR è proprio il titolare. Pertanto si reputa lecito, a partire dagli attributi suggeriti dallo stesso Garante, elaborare un registro che rappresenti a pieno le esigenze e le specificità del proprio Ente.

Di seguito le informazioni che un Titolare deve gestire all'interno del proprio registro dei trattamenti raggruppate in macro sezioni:

- Descrizione trattamento
- Autorizzato
- Finalità
- Tipologia di dati
- Interessati
- Destinatari

- Misure di sicurezza
- Trasferimenti

Generalmente gli attributi da considerare sono:

- **Codice numerico identificativo;**
- **Descrizione trattamento**: indicare sommariamente il tipo di trattamento a cui ci si riferisce;
- **Tipologia di struttura:** tipologia di struttura/dipartimento prevista dall'organizzazione;
- **Dipartimento/Settore/Ufficio/UOA**: tipologia di struttura a cui fa riferimento il trattamento;
- **Finalità e basi giuridiche**: è necessario indicare la finalità per cui si trattano i dati e i Criteri di Liceità su cui si basa il trattamento (Obblighi Contrattuali e pre-contrattuali, Obblighi di Legge, Legittimo Interesse, Consenso dell'interessato, Pubblico Interesse). Buona regola è inserire una sola finalità per ogni trattamento;
- **Denominazione e dati di contatto del Contitolare del trattamento**;
- **Autorizzato al trattamento**;
- **Responsabile del trattamento;**
- **Dati personali**: indicare la tipologia di dato;
- **Dati particolari**: indicare la tipologia di dato;
- **Dati giudiziari**: indicare la tipologia di dato;
- **Termini ultimi di conservazione**: è necessario indicare per quanto tempo vengono trattati i dati prima di cancellarli, tale attributo si definisce attraverso criteri che vanno stabiliti a partire dalle basi giuridiche e finalità legati al principio fondamentale di "minimizzazione", fra i più importanti del Regolamento;
- **Categoria di interessati**: è necessario indicare le categorie a cui si riferiscono i dati (Dipendenti, Utenti sito, Clienti, Fornitori, Candidati, stagisti) ;
- **Categoria di destinatari**: è necessario indicare gli estremi dei Responsabili che trattano i dati per conto del titolare (Medico del lavoro, Centro elaborazione paghe, Web Provider,ecc) e/o eventuali altre Categorie di Titolari a cui possono essere comunicati i dati (Enti Pubblici, Banche, Enti previdenziali);
- **Informativa/consenso**: indicare se previsto dalla norma o meno;
- **Misure di sicurezza**:si indicano le misure di sicurezza adottate per assicurare una protezione adeguata dei dati (pseudomizzazione, cifratura dei dati, back-up,ecc) e possibilmente anche le misure individuate dalla gap analysis e ancora da adottare e i tempi previsti entro cui farlo;
- **Trasferimento dati verso Paesi terzi e Garanzie per il trasferimento**: nel caso i dati possano essere trasferiti in paesi extra UE bisogna indicare quali e, se esistono o meno le condizioni di adeguatezza per questi paesi (es. Privacy

Shield per USA e/o paesi espressamente indicati fra quelli per cui è stata presa una "decisione di adeguatezza" dalla Commissione UE o in base a delle Binding Corporate Rules).

2.4 Compilazione del registro dei trattamenti: il processo

Il procedimento che porta un determinato trattamento all'interno dell'apposito registro segue un iter
classificabile per fasi:

1. **Censimento del trattamento**: scopo dell'attività è quella di capire se vi è una tipologia di trattamento non ancora censita nel registro trattamenti.
2. **Identificazione del trattamento**: scopo dell'attività è identificare i soggetti attivi del trattamento, identificandoli secondo le definizioni del Regolamento.
3. **Verifica di conformità**: scopo dell'attività è capire se il trattamento in esame rispetta in primo luogo i principi di cui all'art. 5 del GDPR ed in seconda battuta le condizioni di liceità di cui all'art. 6.
4. **Valutazione DPIA**: attività che serve ad analizzare una perfetta compliance con il GDPR. Essa si articola in diverse fasi:
   a. Valutazione preliminare: scopo dell'attività è quella di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento è conforme al regolamento GDPR e in seconda battuta comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA.
   b. Esecuzione DPIA: una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti.
   c. Formalizzazione dei risultati: valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva
   d. Eventuale Consultazione Preventiva: consultare l'Autorità di Controllo qualora non sia stato possibile ridurre il rischio residuo a un livello accettabile. L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.
   e. Monitoraggio e Riesame: il processo DPIA, una volta terminate le attività relative alla prima valutazione, deve prevedere un monitoraggio dei risultati raggiunti e un conseguente riesame costante al fine di garantire nel tempo la mitigazione dei rischi e la conformità al Regolamento Europeo anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i

trattamenti. (al termine della valutazione DPIA e prima di passare alla scrittura nel registro dei trattamenti, il DPO deve essere informato e chiamato a valutare il passaggio allo step finale).

5. **Scrittura nel registro trattamenti:** ultima fase del processo è la scrittura del trattamento nell'apposita scheda del registro dei trattamenti mediante allegazione di checklist per l'analisi del rischio.

2.5 Sistema informativo di gestione del registro dei trattamenti

Il registro delle attività di trattamento può essere redatto in formato cartaceo oppure elettronico.
Considerato l'elevato numero di trattamenti censiti che caratterizza l'ente Regione risulta preferibile l'adozione di un sistema informativo che meglio possa rendere l'aggiornamento e/o l'accesso alle informazioni. Ad analoga indicazione si giunge con riguardo ai responsabili esterni che devono essere messi in condizione di potersi censire come tali. Per quanto riguarda inoltre l'aspetto operativo e di implementazione del registro dei trattamenti, è necessario sabilire da subito le linee guida per una corretta gestione degli aspetti formali e di sicurezza. A titolo esemplificativo per esempio si fa riferimento alla necessità di prevedere i log di sistema che consentono di capire quale soggetto ha compiuto determinate azioni, l'archiviazione su una cartella dedicata di un server, prevedere copie di backup settimanali, ecc.
L'implementazione del registro dei trattamenti su sistema informativo avverrà in una seconda fase del progetto, a valle del consolidamento del registro cartaceo e dell'analisi sui requisti funzionali e tecnici che permetteranno di compiere le attività fin qui svolte all'interno dell'Ente, migliorandone l'efficacia e l'usabilità. La Regione Calabria nel corso del 2021 si doterà di un sistema informativo per la gestione informatica del Registro dei Trattamenti.

2.6 Analisi attributo *Autorizzato al trattamento*

E' necessario analizzare l'attributo "Autorizzato al trattamento". Al momento i diversi dipartimenti regionali utilizzano il termine in maniera disomogena. Nello specifico, da una attenta analisi è emerso che nella maggior parte dei casi, veniva esplicitato come "Incaricato al trattamento" il Dirigente del Settore X", per indicare che il personale di quell'ufficio è stato autorizzato a trattare queglli specifici dati. In ottemperanza alle indicazioni/regole interne al dipartimento-settore infatti, in alcuni

trattamenti gli autorizzati sono tutti i dipendenti in quanto è stato considerato che alcune attività- processi riguardino tutti.

Dip	INCARICATO DEL TRATTAMENTO (1)	NORMALIZZAZIONE
01	Dirigente Settore Affari Generali, Giuridici ed Economici e tutto il personale in servizio presso il Settore	Tutti i dipendenti del Settore Affari Generali, Giuridici ed Economici
01	Dirigente Settore Affari Generali, Giuridici ed Economici	Tutti i dipendenti del Settore Affari Generali, Giuridici ed Economici
01	Dirigente e dipenedenti del Settore Segreteria di Giunta e Rapporti con il Consiglio regionale	Tutti i dipendenti del Settore Segreteria di Giunta e Rapporti con il Consiglio Regionale
01	Dirigente Settore Coordinamento	Tutti i dipendenti del Settore Coordinamento Amministrativo dei Dipartimenti
01	Dirigente e dipendenti del Settore Controllo e Repertoriazione decreti dirigenziali	Tutti i dipendenti del Settore Controllo e Repetoriazione Decreti Dirigenziali
01	Dirigente del Settore Ufficio Legislativo e tutti i dipendenti incaricati del trattamento	Tutti i dipendenti del Settore Legislativo
02	RdP, Istruttore, Funzionario addetto	RdP, Istruttore, Funzionario addetto
03	Operatori addetti al protocollo	Dipendenti addetti al protocollo
03	Operatori della gestione PERLA PA	Dipendenti addetti
03	Funzionari addetti	Funzionari addetti
03	Funzionario addetto	Funzionario addetti
03	Dipendenti addetti	Dipendenti addetti
03	Dipendente addetto	Dipendente addetti
03	Funzionari e dipendenti addetti	Funzionari e dipendenti addetti
03	Funzionario	Funzionario addetti
03	Funzionario e un collaboratore	Funzionari e collaboratori
03	Funzionario e collaboratori	Funzionario e collaboratori
03	Collaboratore	Collaboratore

03	Componenti UPD	Dipendenti Ufficio Procedimenti Disciplinari
04	Tutti i Settori del Dipartimento e la Direzione Generale	Tutti i dipendenti del Dipartimento Tutti i dipendenti della Direzione Generale

2.7 Analisi attributo *Tipi di dati personali*

Successivamente si è passati ad analizzare le tipologie di dati censiti nel registro. L'etichetta associata all'attributo dei dati è "Tipi di dati personali" con il quale in modo indistinto si vogliono indicare tutti i dati trattati e si richiede quindi all'utente di specificarne la tipologia.
La nostra attività si è limitata anche in questo caso ad analizzare tutte le "tipologie"di dati censiti e provare a classificarle in tre tipologie di dati differenti:personali, particolari e giudiziari.
Nella prima categoria rientrano i dati relativi alla persona fisica, ovvero:

- dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro)
- situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale.
- dati inerenti lo stile di vita
- situazione economica
- situazione finanziaria
- situazione patrimoniale
- situazione fiscale
- dati di connessione: indirizzo IP, login, altro
- dati di localizzazione: ubicazione, GPS, GSM, altro

Per dati particolari invece si intendono quei dati relativi a:

- Origine razziale ed etnica
- Convinzioni religiose, filosofiche, d'altro genere
- Opinioni politiche
- Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- Stato di salute
- Vita sessuale
- Dati genetici e biometrici

Facenti parte sempre della tipologia di dati particolari, distinguiamo per chiarezza rappresentativa la categoria di dati giudiziari ad esempio: casellario giudiziale, dati relativi a condanne penali e reati).

Di seguito un esempio di come siano stati classificati i dati nelle categorie note.

TIPI DI DATI PERSONALI *(dati tratti dal registro)*
Dati anagrafici, residenza, certificati e referti medici, stato civile, dati giudiziari, dati reddituali

DATI PERSONALI	**DATI PARTICOLARI**	**DATI GIUDIZIARI**
Dati identificativi Dati finanziari	Dati sanitari Stato civile	Dati giudiziari