Autorità di Sistema Portuale
del Mare di Sicilia Occidentale

Porti di Palermo,
Termini Imerese, Trapani,
Porto Empedocle

Autorità di Sistema Portuale del Mare di Sicilia Occidentale

Regolamento per l'attuazione del
Regolamento UE 2016/679 relativo alla
protezione delle persone fisiche con
riguardo al trattamento dei dati personali

(Approvato con Decreto del Presidente n°636 del 2.12.2019)

Art. 1
Oggetto

Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, trattati dall'Autorità di Sistema Portuale del Mare di Sicilia Occidentale (di seguito "AdSP").

Art.2
Titolare del trattamento

L'Autorità di Sistema Portuale del Mare di Sicilia Occidentale, rappresentata ai fini previsti dal RGPD dal Presidente pro tempore, è il Titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Il Titolare adotta misure appropriate per fornire all'interessato:
a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

Il Titolare, inoltre, provvede a:

a) Designare uno o più Responsabili del Trattamento, eventualmente uno per ogni singola struttura in cui si articola l'organizzazione dell'Amministrazione, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;
b) Nominare il Responsabile della Protezione dei Dati (RPD-DPO);
c) Nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione, relativamente alle banche dati gestite da soggetti esterni all'AdSP in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

Art.3
Finalità del trattamento

L'AdSP, Titolare del trattamento, garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto di protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza.
La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale: "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano" (art. 8, paragrafo 1, Carta dei Diritti Fondamentali dell'UE).

Art.4
Responsabile del trattamento

Ai fini del presente regolamento s'intende per "Responsabile" la persona fisica, giuridica, la PA e qualsiasi altro Ente, Associazione ed Organismo che trattano dati personali per conto del Titolare
Il titolare, in considerazione della complessità e della molteplicità delle funzioni dell'Amministrazione, designa quali Responsabili del trattamento di dati personali unicamente i soggetti che presentino garanzie sufficienti per metter in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato (RGPD art.28).

Tutti i soggetti esterni che effettuano operazioni di trattamento sui dati del Titolare "AdSP", per conto e nell'interesse della stessa, per finalità connesse all'esercizio delle funzioni, sono nominati Responsabili del trattamento, qualora siano in possesso dei requisiti di esperienza, capacità ed affidabilità.

I Responsabili del trattamento hanno l'obbligo di:
− Trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia di privacy;
− Rispettare le misure di sicurezza ed adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di

distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
− Trattare i dati personali esclusivamente per le finalità previste dal contratto o dagli obblighi di legge;
− Attenersi alle disposizioni impartite dal titolare del trattamento.

Nel caso di mancato rispetto delle predette disposizioni ne risponde direttamente, verso l'AdSP, il Responsabile del trattamento.

La designazione del Responsabile viene effettuata mediante "atto di nomina" da parte del titolare del trattamento e mediante le Istruzioni operative ivi incluse, da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente al Titolare.

L'accettazione della nomina è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Art.5
Responsabile della Protezione Dati

Il titolare del trattamento designa sistematicamente un responsabile della protezione dei dati (*RPD – Data Protection Officer DPO*).

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 (RGPD).

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 (RGPD);

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
 il Titolare del trattamento;
 il Responsabile del trattamento;
 qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Art.6
Sicurezza del trattamento

L'AdSP e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:
 sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
 dispositivi antincendio; sistemi di rilevazione di intrusione; sistemi di videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di archiviazione sostitutiva documentale; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

L'AdSP e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

I nominativi ed i dati di contatto del Titolare, del Responsabile della Protezione Dati (RDP-DPO) sono pubblicati sul sito istituzionale dell'AdSP, sezione "Amministrazione trasparente"/"privacy" appositamente prevista.

Art.7
Registro delle attività di trattamento

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
− Il nome e i dati di contatto del titolare del trattamento;
− Le finalità del trattamento;
− La descrizione delle categorie di interessati e delle categorie dei dati personali;
− Le categorie dei trattamenti effettuati;
− Le categorie dei destinatari a cui i dati personali sono o saranno comunicati;
− L'indicazione delle misure di sicurezza applicate;
− Eventuale possibilità di trasferimenti di dati all'estero;
− Indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso designato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa dell'Ente in forma telematica/cartacea; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

Il Titolare del trattamento può decidere di affidare al RPD o al "referente interno privacy" il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.
Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Art.8
Consenso al Trattamento dei Dati

Il titolare del trattamento "Autorità di Sistema Portuale del Mare di Sicilia Occidentale" poiché Ente Pubblico (non economico) ha come principale base giuridica del trattamento dei dati la previsione della legge. Non occorre quindi acquisire il consenso da parte dell'interessato purché il trattamento sia previsto per legge, ma soltanto informare gli utenti del trattamento.
Il trattamento è consentito solo per le finalità istituzionali.

Art.9
Valutazioni d'impatto sulla protezione dei dati

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35, pp. 4-6, RGDP.

Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Ente.
Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.
Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

La DPIA non è necessaria nei casi seguenti:
- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre

tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 10
Violazione dei dati personali

Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'AdSP.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.
Il Responsabile del trattamento è obbligato ad informare il Titolare in forma scritta, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

 coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
 riguardare categorie particolari di dati personali;
 comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
 comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
 impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art.11
Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.