ANNO MMXXIII

Autorità di Sistema Portuale
del Mare di Sardegna

Porti di: Cagliari | Olbia | Porto Torres | Oristano | Golfo Aranci | Portovesme | Santa Teresa Gallura | Arbatax

AUTORITÀ DI SISTEMA PORTUALE DEL MARE DI SARDEGNA

PRIVACY POLICY

LINEE GUIDA PER IL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLO SVOLGIMENTO DELLE ATTIVITÀ ISTITUZIONALI DELL'AUTORITÀ DI SISTEMA PORTUALE DEL MARE DI SARDEGNA

Sommario

Linee guida per la tutela della *privacy*
ai sensi del D.Lgs n.196 del 30.06.2003
e del Regolamento (UE) n. 679/2016 (GDPR)
"PRIVACY POLICY"

Lo scopo del presente documento è definire le procedure per adempiere agli obblighi imposti in materia di privacy dal d.lgs. n. 196 del 30.06.2003 (Codice per la protezione dei dati personali – c.d. Codice della Privacy), così come modificato dal d.lgs. n. 101/2018 e del Regolamento (UE) n. 679/2016 (General Data Protection Regulation – c.d. GDPR), tenendo conto delle decisioni e dei provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali, dall'*Article 29 Working Party* (Art. 29 WP) e dall'EDPB (*European Data Protection Board*). In questo modo, si intende fornire uno strumento operativo interno per un corretto trattamento dei dati personali che definisca i ruoli e le responsabilità, nonché gli adempimenti da seguire in materia di protezione dei dati personali.

1. Definizioni.

Ai fini del presente documento si applicano le seguenti definizioni:

Usare una terminologia standard riduce la possibilità di errori.

- **Interessato**: persona fisica a cui i dati personali trattati si riferiscono;
- **dato personale**: qualsiasi informazione riguardante una persona fisica che sia identificata o identificabile (c.d. Interessato); sono quindi dati personali elementi quali il nome, un numero di identificazione, i dati relativi all'ubicazione o all'automobile, il codice fiscale, l'IBAN, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **dati identificativi**: sono i dati personali anagrafici quali il nome, il cognome, l'indirizzo e via dicendo;
- **dati particolari**: sono dati quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, l'orientamento e la vita sessuale, i quali, per loro particolare pervasività nella vita privata dell'Interessato, beneficiano di un sistema di trattamento particolarmente rigoroso. In particolare, tutte le comunicazioni che contengono categorie particolari di dati devono essere effettuate in modo individuale e tale da non farli emergere all'esterno (plico chiuso, PEC con oggetto privo di riferimenti specifici). Sono dati particolari, tra gli altri, i dati genetici, biometrici e sanitari;
- **dati genetici:** 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 e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- **dati biometrici**: dati personali 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 sanitari:** dati personali attinenti alla salute fisica o mentale di una persona fisica, ivi compresi quelli relativi alla prestazione di servizi di assistenza sanitaria. Per la loro elevata incisività sui diritti e le libertà fondamentali, l'AdSP tratta con particolare attenzione i dati sanitari;
- **dati giudiziari:** si tratta di dati personali relativi a condanne penali e reati o a connesse misure di sicurezza. Il loro trattamento può avvenire solo per previsione di legge;
- **finalità del trattamento**: si tratta delle ragioni ultime del trattamento, che prescindono, quindi, da eventuali scopi strumentali. Esse devono essere determinate, esplicite e legittime. Per l'AdSP, le finalità sono esclusivamente quelle predeterminate dalla normativa nazionale ed europea, ossia:
  - svolgere l'attività organizzatoria e concessoria di cui agli art. 16, 17 e 18 L. 84/94, agli articoli da 36 a 55 e 68 c. nav. e relativa alle altre attività commerciali e industriali insistenti nella circoscrizione dell'Ente;
  - assicurare la manutenzione ordinaria e straordinaria elle parti comuni dell'ambito portuale, ivi compreso il mantenimento dei fondali;
  - procedere all'affidamento delle attività legate ai servizi di interesse generale e al relativo controllo su di esse;
  - garantire il coordinamento delle attività amministrative esercitate dagli Enti pubblici nell'ambito dei porti di propria competenza;
  - amministrare in via esclusiva le aree e dei beni del demanio marittimo ricompresi nella propria circoscrizione;
  - assicurare la promozione e coordinamento di forme di raccordo con i sistemi logistici retro portuali e interportuali;
  - garantire la sicurezza degli impianti portuali;
  - salvaguardare, per le aree di competenza, l'integrità ambientale.
- **trattamento**: 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 (v. Operazioni di trattamento);

- **limitazione di trattamento**: il trattamento è limitato quando una o più o la totalità delle operazioni in cui si articola viene temporaneamente o definitivamente preclusa per il futuro;

- **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare, analizzare o prevedere aspetti quali il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di una persona fisica;

- **pseudonimizzazione**: tecnica di cifratura che consiste nel conservare i dati in una forma che impedisce l'identificazione dell'Interessato senza l'utilizzo di informazioni aggiuntive, purché tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative atte a garantirne la conoscibilità solo al Titolare; la pseudonimizzazione si distingue

dall'anonimizzazione, la quale non consente l'identificazione dell'Interessato perché il Titolare non possiede più, o non ha mai posseduto, le informazioni complete. In altre parole, un dato personale anonimizzato non è più leggibile, contrariamente ad un dato pseudonimizzato;

- **procedimento decisionale automatizzato**: consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano; a fronte di ciò, l'Interessato deve essere informato, anche delle possibili conseguenze, e ha il diritto di ottenere l'intervento umano (tenendo eventualmente conto di fattori ulteriori), e di contestare la decisione;

- **archivio:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

- **Titolare del trattamento**: 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, nel caso dell'AdSP, in quanto Ente pubblico, le finalità e i mezzi del trattamento sono determinati dal diritto dell'Unione o degli Stati membri;

- **Contitolare:** Titolare del trattamento distinto dall'AdSP, ma che tratta i dati in maniera congiunta all'AdSP nel determinare finalità e mezzi del trattamento;

- **Nucleo di supporto per le attività di trattamento dei dati personali** (designato): si occupa, ai sensi dell'ordine di servizio del Segretario generale n. 39 del 5 ottobre 2022, del supporto alla gestione operativa degli adempimenti in materia di *privacy*, svolgendo, in particolare, le seguenti funzioni:

  - Studio, proposta e aggiornamento, seguendo gli aggiornamenti in materia e comunicandoli al Titolare;
  - Collaborazione con il DPO;
  - Supporto nella redazione e compilazione delle informative, nella individuazione e nomina degli Autorizzati/Incaricati, all'Amministratore di sistema, anche nella gestione dei sistemi informatici;
  - Assistenza nella prevenzione e gestione degli incidenti di sicurezza, segnalando casi di violazione della *privacy* e contribuendo a garantire la corretta applicazione di specifici provvedimenti emessi dal Garante;
  - Consultazione, mediante partecipazione attiva alle riunioni aventi ad oggetto l'introduzione di una nuova tecnologia e nuove misure sulla sicurezza;
  - Tenuta della documentazione inerente alla *privacy*;

- **Autorizzati/incaricati (addetti istruttoria):** soggetti dipendenti e/o collaboratori dell'AdSP che, dietro formale nomina e previa adeguata formazione, sono autorizzati al trattamento dei dati in base all'incarico ad essi specificatamente conferito;

- **Responsabile della protezione dei dati (DPO):** è il soggetto, diverso dal Titolare, che, dotato di conoscenza specialistica della normativa e delle pratiche in materia di *privacy*, vigila sul corretto adempimento degli obblighi derivanti dal GDPR all'interno dell'Ente e costituisce un punto di contatto interno ed esterno per le questioni rilevanti in materia di *privacy*. L'AdSP attualmente si avvale, a tal fine, di un proprio dipendente in posizione dirigenziale;

Responsabile del trattamento dei dati e Responsabile della protezione dei dati (DPO) sono soggetti distinti e hanno competenze differenti.

- **Responsabile del trattamento**: è la persona fisica o giuridica, l'Ente pubblico, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento; si tratta di una figura esterna all'organizzazione del Titolare, che sussiste allorquando il Titolare affidi ad un terzo lo svolgimento di una o più attività che rientrano nelle proprie competenze, ciò comportando, di conseguenza, lo spostamento del trattamento dei dati inerente le attività affidate. Il Trattamento affidato deve quindi svolgersi nel rispetto delle stesse finalità e degli stessi mezzi stabiliti dal Titolare. Il Responsabile del trattamento può, al più, compiere autonome scelte tecnico-organizzative, purché adeguate a garantire gli standard minimi di sicurezza dettati dal Titolare e nei limiti delle finalità e dei mezzi impostigli. Un Responsabile del trattamento che svolga un trattamento per finalità e mezzi esorbitanti le competenze affidategli diviene, per il trattamento in eccesso, egli stesso Titolare. In Allegato alle presenti Linee guida è riportato uno schema di "Accordo sul trattamento dei dati personali" che può essere adottato dagli Uffici competenti dell'Ente in base alle esigenze che emergono in tal senso;
- **Amministratore di sistema:** è la figura professionale che, in ambito informatico, mantiene, configura e gestisce reti e apparati di telecomunicazione di sicurezza. La nomina ad Amministratore di sistema avviene con l'indicazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. All'Amministratore di sistema compete quindi il rilascio e la custodia delle credenziali di autenticazione per l'accesso alla rete, previa formale richiesta del responsabile d'area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente;
- **Terzo:** la persona fisica o giuridica, l'Ente pubblico, il servizio o altro organismo che non sia l'Interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate/incaricate al trattamento dei dati personali;
- **violazione dei dati personali:** violazione di una misura di sicurezza del trattamento dei dati che comporta distruzione, perdita, modifica, divulgazione o accesso non autorizzati;
- **Autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro con compiti di verifica del rispetto della normativa sulla *privacy*; in Italia è il Garante per la protezione dei dati personali;
- **stabilimento principale:** luogo in cui ha sede l'amministrazione centrale nell'Unione europea e dove avvengono le scelte in termini di finalità e mezzi del trattamento;
- **trattamento transfrontaliero:** poiché nell'AdSP il trattamento dei dati avviene nell'ambito dell'attività di un unico stabilimento, è transfrontaliero il trattamento dei dati che incide, anche solo probabilmente, su Interessati di diversi Stati membri;
- **servizio della società dell'informazione:** qualsiasi servizio prestato, normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale;
- **organizzazione internazionale:** un'organizzazione e gli organismi di diritto internazionale pubblico.

2. Principi, ambito di applicazione e destinatari del regolamento.

L'AdSP si impegna a garantire e dimostrare che il trattamento dei dati avviene in maniera conforme a quanto previsto dalla normativa vigente e secondo i seguenti princìpi:

- **liceità, correttezza e trasparenza**: un trattamento è

  - ✓ lecito solo ed esclusivamente se è giustificato da una delle 6 basi giuridiche elencate nel GDPR: consenso, contratto, obbligo legale, salvaguardia di interessi vitali, interesse pubblico e legittimo interesse;
  - ✓ corretto se è svolto in modo non discriminatorio o comunque pregiudizievole nei confronti dell'Interessato;
  - ✓ trasparente nel momento in cui le comunicazioni sono fatte in modo semplice, comprensibile e inequivocabile;
- **limitazione della finalità**: ogni trattamento deve essere svolto con esclusivo riferimento alle ragioni ultime per le quali è stato posto in essere;
- **minimizzazione dei dati**: i dati trattati in base alla finalità devono essere selezionati tra quelli strettamente necessari, purché adeguati;
- **esattezza**: un trattamento rispondente alle esigenze per cui è attuato necessita di dati costantemente aggiornati ed eventualmente rettificati se inesatti;
- **limitazione della conservazione**: possono essere conservati solo i dati utili al perseguimento di una finalità e per il tempo strettamente necessario così come individuato nell'apposita sezione sul periodo di conservazione dei dati;
- **integrità e riservatezza**: i dati devono essere trattati e custoditi in modo da evitare alterazioni o perdite, anche accidentali (sul punto, si veda la sezione La violazione dei dati personali (Data Breach));
- **responsabilizzazione**: l'AdSP si impegna ad approntare un sistema di trattamento e controlli capace di garantire il rispetto dei precedenti princìpi.

I princìpi generali sono dei veri e propri strumenti di supporto ogniqualvolta vi siano dei dubbi sul trattamento da eseguire.

Detti princìpi, che stabiliscono, in linea di massima approssimazione, che la quantità/qualità dei dati e la modalità del loro trattamento devono essere individuate secondo legge e stretta necessità, devono essere considerati come dei veri e propri strumenti di supporto ogniqualvolta vi siano dei dubbi sul trattamento da eseguire.

Le presenti indicazioni sono valide anche per tutti quei trattamenti di cui l'AdSP è nominata Responsabile del trattamento da altri Titolari, salvo la presenza di misure più restrittive in materia di protezione dei dati personali. La stessa garanzia di protezione e di adozione di adeguate misure di sicurezza è richiesta altresì a quei soggetti terzi ai quali l'AdSP ha affidato l'incarico della gestione dei dati per proprio conto. A tal fine il regolamento sul trattamento dei dati è disponibile presso i Responsabili del trattamento nominati.

3. Le basi giuridiche del trattamento.

Ogni trattamento deve basarsi su una o più delle seguenti basi giuridiche:

- consenso,
- contratto,
- obbligo legale,
- salvaguardia degli interessi vitali,
- interesse pubblico,
- legittimo interesse.

La scelta della base giuridica deve essere effettuata con particolare cautela, in quanto una base inadeguata comporterebbe l'illiceità del trattamento. Inoltre, l'elenco fatto dal GDPR è tassativo, pertanto, non è possibile individuare giustificazioni giuridiche ulteriori.

Per le Pubbliche amministrazioni, inoltre, è fortemente raccomandato evitare il ricorso al consenso e al legittimo interesse. Nel caso si ritenesse di doverli utilizzare, è opportuno consultare preventivamente il DPO.

Capire e applicare correttamente le basi giuridiche è fondamentale per intraprendere un trattamento che sia legittimo.

Contratto.

Sovvertendo in minima parte l'ordine seguito dal GDPR, è bene introdurre le basi giuridiche che legittimano il trattamento partendo dal contratto; pertanto, costituisce una legittima giustificazione il fatto di trattare i dati necessari per l'adempimento di un contratto di cui l'Interessato e il Titolare sono parti oppure per dare seguito alle richieste dell'Interessato in fase precontrattuale.

ESEMPI:

Contratto:

L'AdSP vorrebbe usare i dati del contraente (ad es. un fornitore), sia per la stipula e l'esecuzione del contratto, sia per l'invio di materiale informativo promozionale.

Se riunisse le due finalità (contratto e marketing), chiedendo una sottoscrizione unica, il trattamento non sarebbe legittimo.

Ognuna delle due finalità deve essere distinta:

- la firma del contratto basta per giustificare il trattamento per la stipula e l'esecuzione, mentre
- il consenso per il marketing dovrà essere espresso disgiuntamente.

Ciò significa che, al di fuori di ciò che serve per lo svolgimento dell'attività negoziale (contratto e precontratto), per trattare i dati legittimamente dovrà essere individuata un'altra base giuridica appropriata e ciò vale sia in termini di qualità, sia in termini di quantità di dati e non basta il mero inserimento di una clausola nel contratto per giustificare il trattamento se i dati richiesti non sono strettamente necessari.

In assenza di una valida base giuridica - durante il o alla fine del contratto - i dati dovranno essere cancellati.

La volontà manifestata per il trattamento dei dati ai fini della stipulazione e dell'adempimento di un contratto può essere revocata, ciò comportando, tuttavia, l'impossibilità, dal momento della revoca, di dare corso al medesimo.

Consenso.

È bene prima di tutto tenere a mente che il consenso è, ai fini della *privacy*, concettualmente diverso dal contratto.

Il consenso, infatti, deve essere richiesto per il trattamento di tutti quei dati che non sono strettamente necessari per l'adempimento di un contratto o utili per lo svolgimento dell'attività precontrattuale. Altrimenti detto, quando il Titolare del trattamento intende trattare dati necessari per attività contrattuali (contatto precontrattuale, stipula, adempimento), la base giuridica corretta non è il consenso.

Tuttavia, se in sede di stipula di un contratto (o anche successivamente), si richiedono altri dati per finalità ulteriori (ad es. marketing), che necessitino il consenso, il Titolare deve aver cura di distinguere le due finalità.

Ciò premesso, il consenso consiste in una manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato affinché i suoi dati siano trattati, al di fuori di ciò che necessita per altri fini.

- Il consenso è libero quando non è condizionato e quindi l'Interessato sente di poter manifestare la propria volontà come meglio crede. Il condizionamento, pertanto, deriva da uno squilibrio di potere tra Interessato e Titolare (o Responsabile del trattamento), a sfavore del primo: in questi casi (si pensi ai rapporti con il datore di lavoro), l'Interessato potrebbe verosimilmente subordinare o adeguare la propria volontà a quella del Titolare (o Responsabile del trattamento).
- Il consenso è specifico quando la finalità per cui è richiesto è dettagliata e non vaga o generica.
- Affinché il consenso sia informato è necessario che l'Interessato sia a conoscenza di una serie di elementi fondamentali per il controllo sui propri dati, quali:
  - Identità del Titolare
  - Finalità perseguite con il trattamento
  - Tipologia di dati raccolti e utilizzati
  - Esistenza di un processo decisionale automatizzato
  - Trasferimento dei dati.
- Infine, il consenso è inequivocabile quando sia manifestato in maniera esplicita, mediante azione positiva. Non basta, quindi, una semplice mancanza di dissenso e non serve, d'altro canto, la forma scritta; tuttavia, poiché grava sull'AdSP l'onere di dimostrare di averlo ottenuto e la sua legittimità, è preferibile ottenerlo mediante forma scritta.

ESEMPI:

Consenso:

A seguito di un evento, l'AdSP decide di pubblicare sul proprio sito istituzionale alcune foto che ritraggono i partecipanti.

Poiché non c'è nessun contratto alla base del trattamento (la pubblicazione delle foto), sarà necessario chiedere agli Interessati (i soggetti riconoscibili in foto), un consenso espresso a tal fine.

Poiché nei rapporti con la Pubblica amministrazione è altamente probabile che l'Interessato subisca un condizionamento, è generalmente sconsigliato basare il trattamento sul consenso, il quale difetterebbe del requisito della "libera manifestazione".

L'Interessato può in ogni momento revocare il consenso, lasciando impregiudicato il trattamento avvenuto fino al momento della revoca (tuttavia, si veda il diritto all'oblìo).

Obbligo legale.

I dati devono essere trattati sulla base di un obbligo legale ogniqualvolta vi sia una norma vincolante per il Titolare che non lasci alcuna discrezionalità.

In altre parole, a fronte di una norma che impone un'attività, il Titolare è costretto a trattare i dati necessari per svolgerla. In caso di rifiuto da parte dell'Interessato, l'attività imposta dalla norma non potrà essere svolta e lo stesso Interessato si espone alle conseguenze (anche sanzionatorie), previste dall'ordinamento.

La norma vincolante può sostanziarsi in una legge nazionale o europea, ma altresì in un provvedimento regolamentare proveniente dall'Autorità amministrativa (sono esclusi i regolamenti da soggetti regolatori).

ESEMPI:

Obbligo legale:

L'AdSP può procedere alla stipula di un contratto per lo svolgimento di servizi solo seguendo le prescrizioni del Codice degli appalti, le quali descrivono in modo puntuale ogni passaggio di tutte le fasi dell'attività negoziale pubblica.

Pubblico interesse:

La tutela dei beni del demanio marittimo ricompresi nella circoscrizione dell'AdSP è una finalità di interesse generale che può essere perseguita in vari modi: con la vigilanza, mediante l'implementazione del servizio di pulizia delle aree comuni, dedicando una pagina informativa sul proprio sito istituzionale, consultando i c.d. *stakeholders*, e via dicendo;

Salvaguardia degli interessi vitali.

Allorquando il trattamento dei dati personali si imponga per necessità legate alla salvaguardia della salute o della vita stessa dell'Interessato e nessuna delle altre basi giuridiche possa essere applicata, non occorre alcuna manifestazione di volontà.

Interesse pubblico ed esercizio di pubblici poteri.

Quando, come nel caso dell'AdSP, il titolare persegue uno o più interessi pubblici, ossia volti a beneficio della collettività, il trattamento dei dati si rende necessario per svolgere tutte le attività utili al raggiungimento di tali obiettivi.

Le finalità di interesse pubblico, si noti, devono essere previste dalla legge, nazionale o europea, ma, a differenza dell'obbligo legale, non impongono nello specifico quali attività svolgere e come, bensì solo obiettivi; in altri termini, la differenza tra obbligo legale e interesse pubblico consiste nella possibilità di scegliere le attività da svolgere per raggiungere gli obiettivi, che esiste nel pubblico interesse e non esiste in caso di obbligo legale.

L'Interessato può fare opposizione al trattamento basato sull'interesse pubblico per motivi connessi alla sua situazione particolare, a meno che sussistano giustificazioni inderogabili per il Titolare che prevalgano sugli interessi, sui diritti e sulle libertà dell'Interessato oppure i dati servano al Titolare per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Interesse legittimo.

L'interesse legittimo è un beneficio di varia natura a favore del Titolare, che può legittimare un trattamento di dati se, nel confronto tra gli interessi e i diritti fondamentali dell'Interessato e quelli del Titolare, i secondi prevalgono.

In particolare, per capire se un interesse è legittimo ai fini del trattamento, il titolare deve porsi le seguenti domande:

- Perché si vuole trattare i dati e quali sono i benefici sperati?
- È possibile perseguire i medesimi benefici con modalità meno invasive?
- Il trattamento interferisce con i diritti e le libertà fondamentali dell'Interessato? In quale misura?

Rispondendo a tali domande non si deve ottenere un risultato a sfavore dell'Interessato affinché il trattamento sia legittimo.

L'Interessato può fare opposizione al trattamento basato sull'interesse legittimo per motivi connessi alla sua situazione particolare, a meno che sussistano giustificazioni inderogabili per il Titolare che prevalgano sugli interessi, sui diritti e sulle libertà dell'Interessato oppure i dati servano al Titolare per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'interesse legittimo non può mai giustificare il trattamento di dati particolari.

Ciò premesso, in linea di massima, gli Enti pubblici, e quindi anche l'AdSP, non possono contare sul legittimo interesse per i loro trattamenti, posto che le loro finalità sono stabilite tassativamente dalla legge.

Ragioni legittimanti il trattamento di categorie particolari di dati.

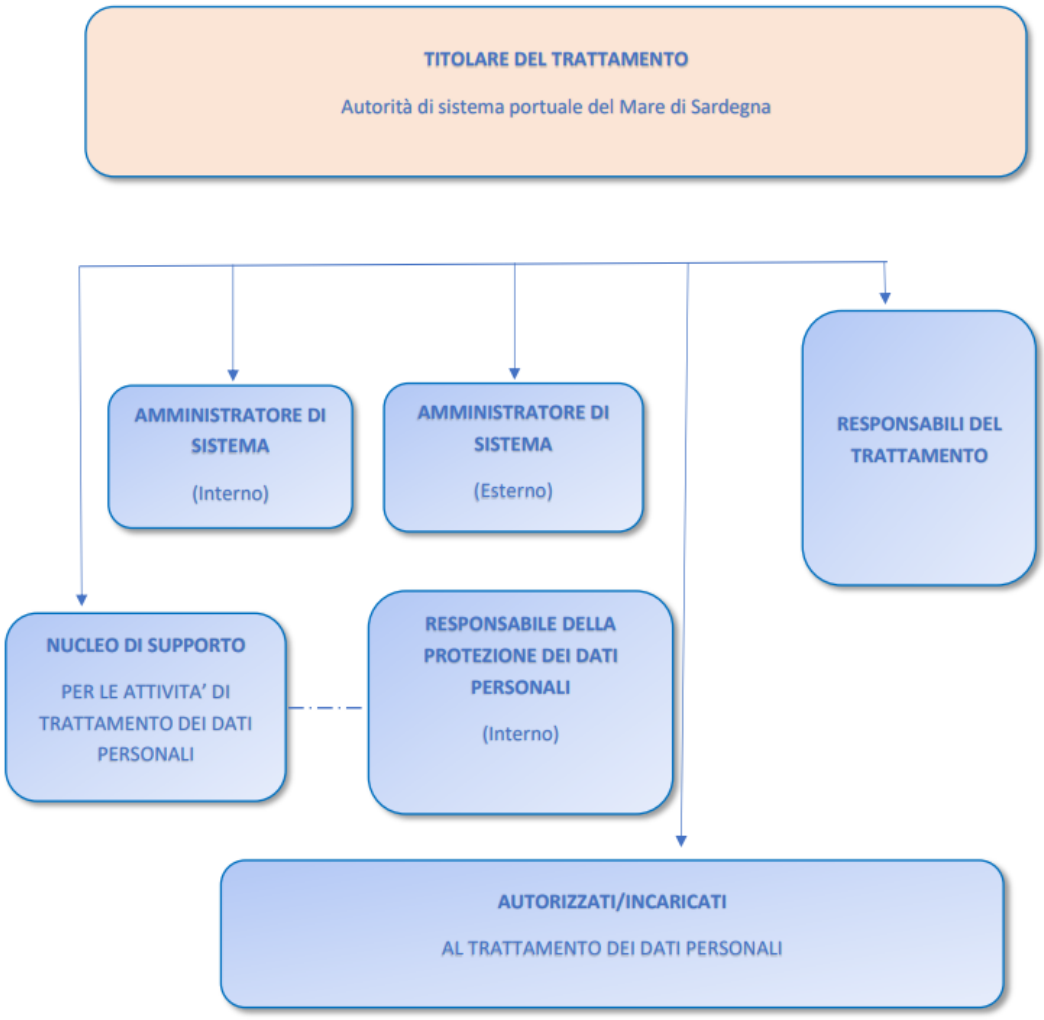
In linea di principio, il trattamento di categorie particolari di dati personali non può essere giustificato da nessuna base giuridica. Tuttavia, il GDPR riconosce che in alcuni casi essi siano imprescindibili per cui prevede una serie di eccezioni che con riferimento all'attività dell'AdSP possono essere così sintetizzate:

- l'Interessato ha prestato il proprio consenso esplicito per una finalità specifica (sempre che la legge non lo vieti);
- il trattamento è necessario per assolvere gli obblighi/esercitare i diritti in materia di diritto del lavoro e della sicurezza sociale;
- è necessario tutelare un interesse vitale dell'Interessato;
- i dati particolari sono già stati resi pubblici dall'Interessato;
- vi è l'esigenza di accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trattamento è legato ad un'attività di interesse pubblico;
- devono essere perseguite finalità di medicina preventiva e del lavoro;
- il trattamento è necessario ai fini di archiviazione nel pubblico interesse.

4. Organigramma della *privacy*.

La mancata conformità alla normativa sulla *privacy* richiede un'attenta adesione alle procedure ed ai contenuti che essa impone e che variano a seconda del ruolo che si ricopre nell'ambito dell'attività svolta dal Titolare.

Una distribuzione chiara e precisa dei ruoli e la sua conoscenza da parte di tutta l'organizzazione emerge dal seguente schema:



5. Registro delle attività di trattamento dei dati personali.

In linea con le prescrizioni del GDPR, l'AdSP ha adottato un Registro delle attività di trattamento svolte sotto la propria responsabilità.

Il Registro del trattamento è un documento contenente informazioni relative al trattamento dei dati personali; tuttavia, non si deve pensare che esso contempli una dettagliata descrizione di ogni singolo trattamento, bensì le informazioni basilari inerenti alle categorie di dati trattati e le caratteristiche delle attività che li coinvolgono.

Per quanto concerne il contenuto, l'AdSP ha scelto di rispettare le prescrizioni minime dettate dal GDPR, specificandole ulteriormente per una migliore e più attenta gestione dei dati; pertanto, il Registro tenuto dall'AdSP contiene le seguenti informazioni:

Parte 1 – Anagrafica Organizzativa:

1. Area dirigenziale: area che procede alla compilazione
2. Ufficio: ufficio che svolge il procedimento (es. Ufficio Legale e Contenzioso)
3. Procedimento di riferimento o di appartenenza: procedimento per il quale sono necessari i dati trattati (ad es. concessione demaniale marittima, appalto di lavori, selezione personale, ricorso, consultazione, etc.)
4. Riferimenti normativi/organizzativi inerenti l'attuazione del procedimento: in questa sezione vanno indicati gli estremi numerici o descrittivi della/e norma/e che giustificano il procedimento di cui al punto precedente (ad es. D. lgs. 50/2016 oppure "Codice degli appalti"; Regolamento d'uso delle aree demaniali marittime; artt. 1218 ss. c.c. oppure "norme sulla responsabilità contrattuale" e via dicendo)
5. Silenzio assenso: indicare se al procedimento si applica l'istituto del silenzio assenso
6. Ambito di applicazione del procedimento: specificare il motivo per il quale il procedimento di cui al punto 3 viene avviato e svolto
7. Base giuridica del trattamento (v. Le basi giuridiche del trattamento.)
8. Provvedimento finale: il provvedimento finale del procedimento ai sensi del punto 3 può consistere in:
   - Decreto presidenziale
   - Delibera del Comitato di gestione
   - Contratto/Affidamento
   - Concessione
   - Autorizzazione
   - Nulla osta
   - Parere
   - Nota formale

   È altresì possibile che nessun provvedimento sia previsto (si pensi ad una pratica di precontenzioso a cui la controparte non dia seguito)
9. Titolare dell'adozione del provvedimento finale:
   - Presidente
   - Comitato di gestione
   - Segretario generale
   - Dirigente
   - Responsabile del procedimento amministrativo
   - Responsabile unico del procedimento

- Non previsto

10. Responsabile del procedimento/ Responsabile unico del procedimento
11. Addetti istruttoria: soggetti che coadiuvano il Responsabile nel procedimento e/o che sono autorizzati/incaricati al trattamento (v. Autorizzati/incaricati)
12. Attori diversi che intervengono nel procedimento: eventuali soggetti terzi autonomi Titolari del trattamento con assunzione diretta delle relative responsabilità (revisori, consulenti, medico del lavoro, assicurazione, ecc.)
13. Interessati (v. Interessati)
14. Categorie di destinatari a cui i dati sono stati o saranno comunicati (ministeri, Enti costituzionali, Enti locali e altri Enti pubblici nazionali, soggetti pubblici europei/internazionali, associazioni di categoria, Enti privati)
15. Soggetti terzi (v. Terzi)
16. Responsabile del trattamento (v. Responsabile del trattamento)
17. Termine finale del procedimento (se non è previsto un termine, ad es. 30 gg. o 3 mesi, indicare un criterio di riferimento indicativo del momento in cui il procedimento verrà chiuso)
18. Termini previsti per la cancellazione dei dati (se non è previsto un termine, ad es. 30 gg. o 3 mesi, indicare un criterio di riferimento indicativo del momento in cui i dati saranno cancellati o resi anonimi: v. periodo di conservazione dei dati).

Parte 2 – Categorie di dati ed operazioni relative ai dati

19,20,21,22. Categorie di dati trattati: questa sezione merita particolare attenzione, poiché la categoria di dati trattati può dettare importanti conseguenze sulle stesse attività di trattamento.
Le categorie che il Registro individua sono:

- Identificativi
- Particolari
- Sanitari (sebbene il GDPR faccia rientrare i dati sanitari tra quelli "particolari", l'AdSP continua a tenere distinta la categoria per questioni di maggiore trasparenza e tutela dei diritti dell'Interessato)
- Giudiziari.

Operazioni di trattamento: la compilazione di questa parte necessita dell'individuazione dell'attività di trattamento che in concreto verrà svolta con specifico riferimento alla micro-finalità di cui al punto precedente. Lo schema seguente costituisce un supporto alla corretta redazione:

Operazione	Descrizione
Raccolta	La raccolta dei dati è la prima operazione e generalmente rappresenta l'inizio del trattamento; consiste nell'attività di acquisizione del dato.
Registrazione	La registrazione consiste nella memorizzazione dei dati su un qualsiasi supporto.
Organizzazione	L'organizzazione consiste nella classificazione dei dati secondo un metodo prescelto.
Strutturazione	La strutturazione consiste nell'attività di organizzazione dei dati secondi criteri specifici per il facile recupero ed un successivo utilizzo.
Conservazione	La conservazione consiste nel mantenere memorizzate le informazioni su un qualsiasi supporto.

Consultazione	La consultazione è la lettura dei dati personali. Anche la semplice visualizzazione dei dati è un trattamento che può rientrare nell'operazione di consultazione
Elaborazione	L'elaborazione consiste nell'attività con la quale il dato personale subisce una modifica sostanziale. La modificazione differisce dall'elaborazione in quanto può riguardare anche solo parte minima del dato personale.
Selezione	La selezione consiste nell'individuazione di dati personali nell'ambito di gruppi di dati già memorizzati.
Estrazione	L'estrazione consiste nell'attività di estrapolazione di dati da gruppi già memorizzati.
Raffronto	Il raffronto è un'operazione di confronto tra dati, sia una conseguenza di elaborazione che di selezione o consultazione.
Utilizzo	L'utilizzo è un'attività generica che ricopre qualsiasi tipo di impiego dei dati.
Interconnessione	L'interconnessione consiste nell'utilizzo di più banche dati, e si riferisce all'impiego di strumenti elettronici.
Blocco	Il blocco consiste nella conservazione con sospensione temporanea di ogni altra operazione di trattamento.
Comunicazione/cessione	La comunicazione (o cessione) consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi, ed è quindi attività particolarmente delicata.
Diffusione	Per diffusione, invece, si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, diffusione anche quando si pubblica online, ad esempio una fotografia su un social network. In assenza di consenso tale attività deve ritenersi illecita.
Cancellazione	La cancellazione consiste nell'eliminazione di dati tramite l'utilizzo di strumenti elettronici.
Distruzione	La distruzione è l'attività di eliminazione definitiva dei dati.

Parte 3 – Modalità di trattamento

23, 24. Piattaforma digitale: nel caso in cui il procedimento non sia supportato solo in modalità cartacea, chiedere all'Amministratore di sistema quale sia la piattaforma utilizzata

25, 26. Software utilizzato: indicare l'applicazione usata nella gestione della pratica; in caso di dubbio, consultare l'Amministratore di sistema

27. Rete aziendale: l'AdSP si avvale di una rete aziendale.

Parte 4 – Minaccia, vulnerabilità ed evento negativo

28 e seguenti.

Descrizione minaccia	Descrizione vulnerabilità	Misure di mitigazione adottate o da adottare per mitigare i rischi
Accesso non autorizzato: accesso ai dati da parte di soggetti (interni o esterni) non aventi diritto	Armadi aperti/computer non protetti da password in locali dove è possibile l'accesso di terzi o di personale interno non autorizzato	Conservare il dato in armadi chiusi, accessibili solo a Dirigente, Responsabile e Addetti istruttoria. Lasciare i computer spenti, o in stand by muniti di password sicura. Conservare le password in luogo protetto e inaccessibile.
Indisponibilità temporanea dei dati	Arresto anomalo del sistema. Malfunzionamento della rete. Possibile mancata erogazione energia elettrica.	Munire gli edifici e/o i dispositivi di un gruppo di continuità. Dotare l'ente di un server di supporto e backup.
Indisponibilità permanente e irreversibile dei dati.	Perdita e/o distruzione dei supporti di memorizzazione e archiviazione materiali e/o digitali	Dotare l'ente di un server di supporto e backup. Collocare l'archivio documentale in luoghi protetti adatti a garantire l'integrità degli stessi. Digitalizzare i documenti cartacei.
Indebita comunicazione: comunicazione (fortuita o intenzionale) dei dati verso terzi non autorizzati.	Utilizzo di reti non sicure. Errori nella digitazione indirizzi. Comportamenti soggetti interni/esterni con cui l'Ente entra in contatto.	Lavorare esclusivamente con piattaforme sicure. Adeguata formazione e responsabilizzazione dei soggetti interni/esterni.
Alterazione: modifica impropria	Armadi aperti/computer non protetti da	Conservare il dato in armadi chiusi, accessibili solo a Dirigente, Responsabile e Addetti istruttoria. Lasciare i computer spenti, o in stand by muniti di password sicura.

(accidentale o intenzionale) dei dati	password in locali dove è possibile l'accesso di terzi o di personale interno non autorizzato. Comportamento del personale dipendente.	Conservare le password in luogo protetto e inaccessibile. Adeguata formazione e responsabilizzazione dei soggetti interni/esterni.
Diffusione: divulgazione impropria di informazioni riservate	Comportamento del personale dipendente. Salvataggio inadeguato dei dati. Collocamento delle postazioni di lavoro.	Conservare il dato in armadi chiusi, accessibili solo a Dirigente, Responsabile e Addetti istruttoria. Lasciare i computer spenti, o in stand by muniti di password sicura. Conservare le password in luogo protetto e inaccessibile. Adeguata formazione e responsabilizzazione dei soggetti interni/esterni.
Monitoraggio continuo: controllo ininterrotto e indiscriminato delle informazioni.	Comportamenti soggetti interni/esterni con cui l'Ente entra in contatto.	Limitare l'accessibilità ai dati predeterminando le situazioni che la giustificano ed i soggetti abilitati.

Su richiesta, il Titolare del trattamento o il Responsabile del trattamento mettono il Registro a disposizione dell'Autorità di controllo.

6. Diritti degli Interessati.

Il GDPR predispone a tutela degli Interessati una serie di diritti inderogabili, che possono essere esercitati in qualsiasi momento previa identificazione - e quindi non in forma anonima - con una semplice richiesta all'AdSP.

L'AdSP è tenuta a dare seguito alla richiesta in modo gratuito e senza ritardo, tenendo conto della fondatezza, della complessità e del numero delle richieste; in caso di richiesta manifestamente infondata o eccessiva, l'AdSP può addebitare un contributo spese o rifiutarla.

Diritto di accesso.

Nel rispetto dei diritti e delle libertà altrui l'Interessato può chiedere all'AdSP, previa conferma dell'esistenza del trattamento, informazioni circa:

- Le finalità del trattamento
- I dati trattati
- Il soggetto a cui vengono eventualmente trasmessi i dati
- Il periodo di conservazione dei dati
- Quali diritti possono essere esercitati e verso chi

- Le informazioni sulle eventuali modalità automatizzate del trattamento o sulla profilazione.

L'accesso può essere esercitato entro il **periodo di conservazione dei dati**, ossia:

- I dati personali relativi a contratti stipulati con l'AdSP devono essere accessibili agli Interessati per tutta la durata del contratto (dall'attività precontrattuale fino alla completa esecuzione) e, successivamente, per il periodo in cui vige la garanzia sui beni/servizi prestati.

  Tutti i dati hanno una "scadenza", nel senso che essi devono essere trattati per lo stretto necessario in termini di finalità e tempi.

  Inoltre, i dati inerenti all'attività negoziale devono essere conservati e resi disponibili per il periodo necessario all'adempimento degli obblighi tributari, fiscali, previdenziali e assistenziali. Per la fatturazione e le scrittura contabili la legge prevede un periodo di conservazione di 10 anni dalla data di emissione della fattura o dall'ultima registrazione.

  Il fascicolo del dipendente e i cedolini devono essere conservati per un periodo di 5 anni dall'ultima registrazione.

  Nel caso in cui si dovesse instaurare un contenzioso, i dati sono conservati e di conseguenza devono essere accessibili per tutta la durata della vertenza e per 5 anni dalla sua conclusione.

  I dati personali relativi ai singoli partecipanti alle procedure selettive devono essere conservati e resi accessibili per il periodo di validità delle graduatorie previsto dalla normativa vigente.

- I dati trattati al fine del rilascio di licenze/autorizzazioni devono essere accessibili agli Interessati per tutta la durata della licenza/autorizzazione.

  Inoltre, i dati inerenti l'attività derivante dalla licenza/autorizzazione devono essere conservati e resi disponibili per il periodo necessario all'adempimento degli obblighi tributari e fiscali.

  Nel caso in cui si dovesse instaurare un contenzioso, i dati sono conservati e di conseguenza devono essere accessibili per tutta la durata della vertenza e per 5 anni dalla sua conclusione.

- I dati oggetto di videoripresa devono essere conservati e resi accessibili per un periodo non superiore ai 5 giorni, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità giudiziaria o di Polizia giudiziaria.

  È importante mettere in evidenza che l'accesso a dati video/fotografici potrebbe comportare la diffusione di dati riguardanti altri soggetti, diversi dall'Interessato. Questo pone il problema della corretta gestione degli accessi.

  Posto che la protezione di diritti di terzi non può essere usata come pretesto per impedire legittime richieste di accesso, in questi casi:

- se la richiesta di accesso è circostanziata nello spazio e nel tempo può essere sufficiente mascherare o crittografare le immagini in modo da rendere non riconoscibili i terzi presenti nell'inquadratura;
- se, invece, la richiesta comprende un lasso di tempo e/o un ambito spaziale ampio o addirittura indeterminato per cui sarebbe necessaria un'attività di indagine per rinvenire le immagini e l'Interessato non riuscisse a fornire elementi utili per limitare l'accesso, occorre indirizzarlo verso soggetti dotati dei poteri necessari a tal fine.

La protezione di diritti di terzi non può essere usata come pretesto per impedire legittime richieste di accesso

- Nel caso in cui i dati siano conservati per finalità di archiviazione, laddove possibile essi devono essere resi anonimi e quindi non accessibili; ove, invece, ciò non avvenga, l'accessibilità è garantita per tutto il periodo in cui vige l'obbligo di tenuta dell'archivio.

Diritto di rettifica.

Posto che i dati personali trattati devono essere esatti e tenuti aggiornati dall'AdSP, essi devono altresì essere tempestivamente rettificati e integrati su richiesta dell'Interessato con immediata comunicazione agli eventuali destinatari dei dati (v. Diritto di notifica).

Diritto di cancellazione.

Quando i dati non sono più necessari, sono trattati in modo illecito oppure tutte le volte in cui la legge lo preveda, l'Interessato può chiederne la cancellazione con immediata comunicazione agli eventuali destinatari dei dati (v. Diritto di notifica).

Rendere i dati definitivamente non riferibili ad una persona fisica equivale alla cancellazione.

L'offuscamento delle immagini, l'anonimizzazione e ogni altra forma di intervento sul dato che lo renda definitivamente e irreversibilmente non riferibile, neppure in via indiretta, ad una precisa persona fisica, equivale alla cancellazione.

Diritto all'oblio.

Se i dati di cui viene richiesta la cancellazione sono stati resi pubblici, si pone una questione di "diritto all'oblio" dell'Interessato, ossia del diritto di essere dimenticati: per questo motivo, ove l'AdSP avesse diffuso pubblicamente dei dati come spesso accade mediante la pubblicazione sul sito istituzionale, oltre a provvedere all'immediata cancellazione, essa deve tempestivamente informare eventuali altri Titolari del trattamento della necessità di cancellare qualsiasi link, copia o riproduzione dei dati.

Diritto di limitazione del trattamento.

Qualora l'Interessato ritenesse che i dati personali non siano corretti oppure reputasse il trattamento in parte illecito o, ancora, se i dati non fossero più necessari per le finalità iniziali, ma l'AdSP dovesse averne bisogno in sede giudiziale (e quindi non può cancellarli), l'Interessato può ottenere che il trattamento sia svolto in modo limitato a determinati dati e/o mezzi e modalità con immediata comunicazione agli eventuali destinatari dei dati (si veda Diritto di notifica).

Quando si applica la limitazione al trattamento (qualunque sia la forma scelta), i dati limitati devono essere trattati soltanto con il consenso dell'Interessato, a meno che non debbano essere semplicemente conservati.

Il consenso non è necessario se il dato limitato serve all'AdSP per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziale oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico.

La revoca della limitazione deve essere preventivamente comunicata all'Interessato.

Diritto di notifica.

Ogniqualvolta vi sia un'attività di rettifica, cancellazione o limitazione del trattamento, è necessario comunicarlo tempestivamente a tutti i destinatari dei dati, a meno che ciò sia impossibile o comporti uno sforzo sproporzionato.

L'impossibilità di notifica è da intendersi in senso assoluto e deve essere dimostrata.

L'impedimento temporaneo non è un'impossibilità, pertanto, laddove sia necessario, la notifica deve essere semplicemente differita.

Lo sforzo è sproporzionato se le esigenze di notifica potrebbero essere soddisfatte solo con un impegno tale da paralizzare l'attività dell'ente, oppure rendere inefficiente lo svolgimento delle attività istituzionali previste a beneficio della collettività.

In questi casi la notifica può essere differita temporaneamente.

Le generalità dei destinatari dei dati devono essere rese note all'Interessato a semplice richiesta.

Diritto di opposizione.

L'Interessato ha il diritto di opporsi al trattamento per motivi connessi alla sua situazione particolare, quando:

- il trattamento sia necessario per l'esercizio di un'attività volta al perseguimento di un interesse pubblico;
- qualora i dati personali siano trattati per finalità di marketing;
- se i dati personali sono trattati per fini statistici non legati all'esecuzione di un compito di interesse pubblico.

L'opposizione potrà non essere accolta dall'AdSP qualora sussistano motivi legittimi inderogabili per procedere al trattamento che prevalgono sugli interessi dell'Interessato.

In particolare, in caso di dati inerenti la videosorveglianza, l'opposizione potrà essere fatta valere alle seguenti condizioni:

- nelle aree videosorvegliate liberamente accessibili, l'AdSP possa interrompere il trattamento (la videoripresa), immediatamente a seguito della richiesta;
- nelle aree videosorvegliate ad accesso limitato per questioni di *security*, invece, in caso di opposizione non potrà essere consentito l'accesso all'Interessato.

L'opposizione è esclusa in caso di obbligo legale e di contratto.

Ciò non significa che all'Interessato sia impedito rendere i propri dati indisponibili: i dati personali sono un bene che rimane sempre e comunque nella piena disponibilità dell'Interessato. Tuttavia, quando un trattamento dei dati deriva da una disposizione vincolante in virtù di un obbligo legale o contrattuale (il contratto è "legge" tra le parti), se i dati venissero resi indisponibili con un'ipotetica opposizione, si verrebbe meno alla possibilità di rispettare il vincolo che ne deriva e l'Interessato si esporrebbe all'applicazione delle sanzioni previste di conseguenza dall'ordinamento.

I dati personali sono un bene che rimane sempre e comunque nella piena disponibilità dell'Interessato

Di fronte ad una richiesta dell'interessato, l'AdSP è legittimata a limitare l'esercizio dei diritti sopra elencati in base a previsioni di legge a tutela di interessi superiori quali la sicurezza nazionale, la difesa, la sicurezza pubblica, la prevenzione, l'accertamento e la persecuzione di reati, l'esercizio di pubblici poteri, la difesa dei diritti dell'interessato o dei diritti e delle libertà altrui, l'esercizio di azioni civili, e, in particolare:

- gli interessi tutelati dalle disposizioni in materia di riciclaggio e di sostegno alle vittime di richieste estorsive;
- l'attività di Commissioni parlamentari d'inchiesta;
- le attività svolte da Enti pubblici in materia di politica monetaria e valutaria, sistema dei pagamenti, intermediazione e mercati creditizi e finanziari;
- lo svolgimento di investigazioni difensive e l'esercizio di un diritto in sede giudiziaria;
- la riservatezza dell'identità del dipendente che segnala un illecito di cui sia venuto a conoscenza in ragione del proprio ufficio;
- la prevenzione e il contrasto dell'evasione fiscale.

Il rigetto della richiesta deve essere motivato ed espresso in forma scritta.

7. Informazione degli Interessati.

Affinché un trattamento sia legittimo esso deve essere reso noto all'Interessato, anche quando non è necessario acquisire il consenso, semplicemente, perché l'esercizio dei diritti verso il Titolare implica la conoscenza del trattamento e delle sue caratteristiche.

Per questo motivo, l'AdSP ha reso pubblicamente consultabili, tramite il proprio sito istituzionale, cinque informative specifiche. È possibile accedere alle stesse attraverso il seguente link:

https://www.adspmaredisardegna.it/amm-trasparente/privacy-policy/

È obbligatorio fornire sempre l'informativa appropriata all'Interessato, anche qualora non dovesse essere sottoscritta.

All'interno di ogni singola informativa sono riportate in modo semplice e chiaro tutte le informazioni inerenti l'attività di trattamento (Titolare del trattamento, Responsabile per la protezione dei dati, finalità e modalità del trattamento, diritti dell'Interessato, eventuale trasferimento a terzi, categorie di dati particolari trattati, base giuridica). Nel rispetto delle previsioni del GDPR, autorizzati/incaricati hanno l'onere di acquisirne conoscenza anche in merito al contenuto, affinché esse possano essere rese anche oralmente, in caso sia necessario.

Informativa generale.

Durante lo svolgimento della propria attività istituzionale, l'AdSP può venire a conoscenza di dati che riguardano utenti che occasionalmente si recano presso le sedi dell'AdSP e negli ambiti territoriali di sua competenza o che visitano il sito istituzionale. Per tali eventualità l'AdSP si impegna, mediante un'apposita informativa a carattere generale, al fine di garantire il rispetto della normativa sulla *privacy*.

Informativa relativa al trattamento dei dati personali tramite videosorveglianza.

In considerazione del fatto che l'area di competenza dell'AdSP è sottoposta a videosorveglianza per finalità di sicurezza degli impianti portuali e salvaguardia del patrimonio e dell'ambiente, è disponibile sul sito istituzionale un'informativa che espone le modalità di acquisizione, conservazione e gestione dei dati raccolti tramite videoriprese, nonché dei diritti degli Interessati.

L'informativa sulla videosorveglianza è liberamente consultabile sul sito istituzionale dell'AdSP, anche mediante lettura dei codici QR riportati dalla cartellonistica posizionata in prossimità delle videocamere.

Un richiamo mediante collegamento alla stessa informativa deve altresì essere inserito in ogni contratto di cui l'AdSP sia parte (fornitori, dipendenti, soggetti operanti in porto).

Informativa negoziale.

L'AdSP tratta i dati personali di coloro con cui intraprende contatti prenegoziali e/o stipula contratti (appalti, servizi, concessioni, licenze, autorizzazioni), al fine di procedere alla stipula e all'esecuzione dei medesimi e a tutte le attività preparatorie (selezione pubblica) e conseguenti (eventuali azioni in garanzia o giudiziali, oppure scorrimento di graduatorie).

L'attività prenegoziale e negoziale in questione è comunque da riferire a quella derivante dagli obblighi istituzionali dell'AdSP; tuttavia, posto che il trattamento dei dati può estendersi ad aspetti legati alla comunicazione promozionale, l'informativa negoziale deve essere fatta sottoscrivere alla controparte e allegata alla documentazione contrattuale.

Informativa dedicata ai soggetti operanti in porto.

Per coloro che facciano istanza di licenza ex art. 16 e 17 l. 84/94 e di iscrizione nei registri di cui all'art. 68 c. nav. è stata predisposta un'apposita informativa.

L'informativa dedicata ai soggetti operanti in porto non necessita di sottoscrizione, ma è opportuno che si abbia prova della presa visione da parte degli operatori, ragione per la quale è necessario che essa sia allegata ai documenti da compilare per la presentazione dell'istanza.

Informativa per i dipendenti.

L'AdSP, al fine di adempiere ai propri obblighi di gestione del personale, raccoglie i dati dei propri dipendenti ed eventuali collaboratori informandoli dei propri diritti.

L'informativa per i dipendenti deve essere sottoscritta ed allegata al fascicolo personale del dipendente.

8. La violazione dei dati personali (*Data Breach*).

La violazione dei dati personali è una probabile conseguenza di un incidente di sicurezza, ossia di un evento, accidentale o meno, che comprometta uno o più (congiuntamente o separatamente), dei seguenti aspetti:

- riservatezza dei dati (divulgazione, accesso non autorizzato)

ESEMPI:

Per prevenire un *data breach*, l'eventuale passaggio di consegna tra dipendenti di un dispositivo (PC, tablet, smartphone, e via dicendo), deve essere preceduto da un'attenta formattazione, mentre la cessione a terzi esterni all'organizzazione è da escludere tassativamente.

I dispositivi dismessi devono essere distrutti.

- integrità dei dati (alterazione, modifica)
- disponibilità (perdita, distruzione, impossibilità temporanea o definitiva di accedere).

Si noti che, benché la formula "incidente di sicurezza" possa far pensare in prima battuta ad attacchi provenienti dall'esterno a danno del Titolare, anche un trattamento eseguito all'interno che accidentalmente non rispetti le regole di conformità alla *privacy* può esserlo.

Inoltre, l'eventuale indisponibilità temporanea programmata (ad es. per motivi di manutenzione o aggiornamento), non costituisce in sé una violazione della sicurezza.

In via preventiva, al Titolare compete di:

- adottare tutte le misure necessarie e approntare procedure interne efficaci per venire a conoscenza tempestivamente di eventuali violazioni e porvi rimedio
- coinvolgere tutti i dipendenti/collaboratori nella formazione in materia di *privacy*, sin dal momento dell'assunzione, predisponendo linee guida, assistenza e aggiornamento;
- disporre accordi con i Responsabili del trattamento di cui eventualmente si avvale.

ESEMPI:

Una delle attività che espone maggiormente a incidenti di sicurezza è la navigazione sul web per attività estranee a quella lavorativa (consultazione di pagine social o di caselle mail personali, tra le altre), l'utilizzo di hotspot personali e di dispositivi di archiviazione non autorizzati (usb drive, hard disk esterni).

È dunque opportuno astenersi dai predetti comportamenti.

È fondamentale che dipendenti/collaboratori diano adeguata importanza ad ogni comunicazione dell'AdSP in materia di privacy, partecipino agli eventi formativi e manifestino tempestivamente ogni dubbio o incertezza.

Quando si verifica una violazione dei dati, gravano sul Titolare tre categorie di obblighi:

- obblighi di notifica al Garante e agli Interessati
- obblighi di intervento
- obblighi di registrazione.

Obblighi di notifica.

Il Titolare è obbligato a comunicare la violazione sia al Garante, sia agli Interessati, ove sia probabile che si verifichino effetti negativi.

La comunicazione deve essere fatta dal momento in cui il Titolare ne ha conoscenza, ossia è ragionevolmente sicuro del fatto che vi è stata una violazione:

- al Garante, qualora essa abbia probabili effetti negativi sui diritti e le libertà degli Interessati: entro 72h; in caso di ritardo, devono essere allegate idonee giustificazioni
- agli Interessati, qualora essa abbia possibili effetti negativi sui diritti e le libertà degli Interessati: da effettuare senza ingiustificato ritardo.

Peraltro, non vi è un ordine cronologico tassativo, per cui, se le indagini necessarie per la notifica al Garante fossero tali da richiedere del tempo, potrebbe verosimilmente essere compiuta per prima la comunicazione agli Interessati.

Si noti che nel caso la violazione sia rilevata da un eventuale Responsabile del trattamento, questi ha solo l'onere di notificarla al Titolare senza ritardo, senza dover svolgere alcuna valutazione in merito all'incidenza sui diritti e le libertà dell'Interessato, valutazione che invece grava sul Titolare.

Nella comunicazione all'Autorità di controllo devono essere indicate:

- la natura della violazione e, ove possibile, le categorie di dati e il numero (anche approssimativo) degli Interessati a cui fanno riferimento;
- le probabili conseguenze;
- le misure adottate o di cui si propone l'adozione.

Laddove non sia possibile compiere una comunicazione esaustiva nell'immediatezza, può essere fatta una comunicazione "per fasi", indicando i motivi di tale scelta all'atto della prima notifica.

La comunicazione al Garante può altresì contenere richieste di informazioni o proposte operative relative alla violazione che ne è oggetto.

Nella comunicazione agli Interessati è necessario indicare:

- la natura della violazione
- nome e contatti del DPO
- le probabili conseguenze
- le misure adottate o di cui si propone l'adozione

provvedendo alla notifica personale, ovvero, laddove ciò richieda uno sforzo sproporzionato, usando metodi alternativi e anche mediante diversi mezzi simultaneamente.

La procedura di notifica può essere svolta tramite l'apposita sezione del sito del Garante della *privacy* all'indirizzo https://servizi.gpdp.it/databreach/s/ e deve essere curata dal Nucleo di supporto per le attività di trattamento dei dati personali, al quale chiunque abbia anche solo un dubbio circa l'evenienza deve fare tempestivo riferimento; il Nucleo di supporto per le attività di trattamento dei dati personali può coinvolgere il DPO per le valutazioni del caso.

Obblighi di intervento.

Il Titolare, in caso di un *data breach*, è tenuto ad approntare ogni misura tecnica e organizzativa per farvi fronte, oltre che in termini di notifica, in termini di prevenzione e/o contenimento delle conseguenze.

Obblighi di registrazione.

Il Titolare è tenuto a conservare la documentazione relativa a ogni violazione avvenuta, anche non notificabile, e a redigere un apposito Registro dei *data breach* in cui annotare ogni loro dettaglio nonché la descrizione delle valutazioni alla base delle decisioni adottate.

9. Le conseguenze della violazione della *privacy*. Sanzioni e responsabilità.

Il rispetto della normativa vigente sulla *privacy* e delle linee guida che ne derivano trova fondamento nella necessità di tutelare l'Interessato, il quale subisce il rischio di un'indebita intrusione nella propria sfera personale.

Questa tutela beneficia di un rinforzo in termini dissuasivi che va ben oltre lo stesso GDPR e consiste in un pesante apparato sanzionatorio amministrativo, civile, penale ed erariale.

Responsabilità amministrativa.

Le sanzioni amministrative sono quelle previste per la violazione del GDPR ed emesse dal Garante per la *privacy* a carico del Titolare del trattamento (l'AdSP), dell'eventuale Responsabile del trattamento e dell'eventuale organo di certificazione nei seguenti casi:

1. violazioni relative alle modalità di esecuzione del trattamento dati prescritte dal GDPR, ad esempio:
    - non si è tenuto correttamente il Registro del trattamento
    - non si è provveduto alla nomina del DPO
    - si è omessa la valutazione d'impatto DPIA
    - si è omessa la notifica di un *data breach.*

In questi casi è prevista un'ammenda fino a 10 milioni di euro.

2. Violazioni ai principi generali stabiliti dal GDPR, ossia:
    - assenza del consenso al trattamento
    - violazione dei diritti dell'Interessato
    - mancanza o inidoneità dell'informativa sulla *privacy*
    - violazione delle disposizioni circa il trasferimento dei dati a Paesi Terzi.

La violazione della normativa sulla privacy può dare luogo a responsabilità su tutti i piani giuridici:

amministrativo, civile, penale ed erariale.

Queste violazioni della *privacy* prevedono una multa fino a 20 milioni di euro.

Il Garante ha altresì il potere di imporre una serie di correttivi (limitazione/divieto, sospensione del flusso dei dati), che potrebbero comportare un blocco operativo del Titolare, con tutte le conseguenze che ne deriverebbero e le relative responsabilità.

Responsabilità civile.

Le violazioni della *privacy* possono comportare anche un danno per l'Interessato i cui dati sono stati trattati illegittimamente. In questo caso l'Interessato può chiedere in sede civile il risarcimento al Titolare e all'eventuale Responsabile del trattamento, salvo che essi dimostrino che la causa del danno non è ad essi imputabile. Si noti peraltro che sebbene l'azione davanti al giudice nazionale sia alternativa al reclamo dinanzi al Garante

- il Garante è comunque informato dei giudizi di cui non è parte e formula osservazioni;
- l'Interessato che riceva una decisione favorevole del Garante ha la possibilità di agire successivamente in sede civile per il risarcimento dei danni e che il provvedimento del Garante ha natura di "prova privilegiata" per l'accertamento della violazione da parte del giudice.

Il risarcimento del danno non può essere chiesto al DPO**,** perché il DPO ha responsabilità contrattuale solo verso il Titolare del trattamento.

Le responsabilità derivanti da violazioni nel trattamento dei dati possono coinvolgere tutti i livelli dell'Ente, dai Dirigenti agli autorizzati/incaricati.

Responsabilità penale.

Violare la *privacy* può altresì essere penalmente rilevante nei seguenti casi:

- trattamento illecito dei dati personali; se il trattamento riguarda dati trattati "su larga scala" l'infrazione è più grave;
- acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala;
- falsità nelle dichiarazioni fatte al Garante;
- inosservanza delle disposizioni e delle autorizzazioni del Garante (in particolare, per quanto concerne l'attività dell'AdSP, rileva l'Autorizzazione Generale n. 1/2016 sul trattamento dei dati sensibili nei rapporti di lavoro);
- violazione della riservatezza dei dipendenti da parte del datore di lavoro in due casi particolari:
    - utilizzo di strumenti di controllo a distanza quando non ci sono le esigenze produttive o organizzative, o comunque senza le dovute autorizzazioni;
    - indagini su dipendenti o candidati all'assunzione su fatti non rilevanti ai fini dell'attività lavorativa.

Le sanzioni penali sono concordate fra il Pubblico Ministero e il Garante per la *privacy* e ricadono non già sull'Ente, ma sull'autore dell'illecito, quindi, eventualmente, anche un autorizzato/incaricato.

Responsabilità erariale.

In generale, si osserva che il dovere di conformità al GDPR deve essere osservato a tutti i livelli organizzativi e fatto oggetto di puntuale controllo da parte dei dirigenti, posto che le eventuali violazioni sono fonte di responsabilità personale presupposto per la configurabilità del danno erariale.

10. Strumenti di tutela a disposizione dell'Interessato.

In un'ottica di gradualità e differenziazione della tutela dell'Interessato, i procedimenti che possono instaurarsi sono quelli descritti di seguito.

1. L'Interessato formula personale istanza per l'esercizio di uno o più diritti presso il Titolare, il quale è tenuto a rispondere senza ingiustificato ritardo e al più tardi entro un mese dal ricevimento della richiesta (tale termine può essere prorogato di 2 mesi, qualora si renda necessario per via della complessità e del numero di richieste, previa comunicazione all'interessato entro 1 mese dal ricevimento della richiesta). Non è previsto il silenzio rigetto.
   Se il Titolare non fornisce le informazioni o esse non soddisfano le richieste dell'Interessato, quest'ultimo può rivolgersi al Garante scegliendo tra segnalazione e reclamo, entrambi gratuiti.

Segnalazione e reclamo sono rimedi esperibili davanti al Garante della Privacy in via del tutto gratuita e con tempi di svolgimento molto brevi.

2. La segnalazione è una semplice denuncia non circostanziata che invita il Garante ad effettuare un'attività di controllo sul trattamento che si ritiene illecito; la segnalazione non comporta necessariamente l'adozione di un provvedimento da parte del Garante.
   Il reclamo, invece, è un atto circostanziato e quanto più dettagliato possibile, sottoscritto digitalmente o con firma autenticata, con cui l'Interessato comunica al Garante una precisa violazione della normativa *privacy*. Il Garante è tenuto a rispondere entro 90 giorni.

   Sia la segnalazione, sia il reclamo, possono essere presentati per raccomandata o via PEC agli indirizzi protocollo@gdpr.it oppure protocollo@pec.gdpr.it

3. Contro la decisione del Garante in sede di reclamo può essere presentato ricorso davanti al giudice civile entro 30 giorni dalla comunicazione (60 giorni se il ricorrente risiede all'estero), a pena di inammissibilità. I tempi sono quelli della giustizia ordinaria e la sentenza non è appellabile, ma può essere oggetto di ricorso in Cassazione.

L'Interessato ha altresì:

4. il diritto di rivolgersi al giudice ordinario (civile o penale), qualora ritenga che i propri diritti in tema di *privacy* siano stati violati, in alternativa ad un reclamo;

5. il diritto di chiedere il risarcimento davanti al giudice civile, sia in alternativa, sia in conseguenza ad un reclamo, per i danni subìti dal trattamento al Titolare o al Responsabile del trattamento, salvo che essi dimostrino che l'evento dannoso non è ad essi imputabile.

****

Allegati:

1. **Schema di Accordo sul trattamento dei dati personali (ADP);**
2. **Addendum sui cookies ed altri strumenti di tracciamento.**

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

Il presente Accordo sul trattamento dei Dati Personali ("**ADP"**) viene stipulato tra:

(i) l'**Autorità di sistema portuale del Mare di Sardegna**, con sede in Cagliari (CA), Molo Dogana s.n.c., rappresentato dal Prof. Avv. Massimo Deiana, in qualità di Presidente dell'Autorità di sistema portuale del Mare di Sardegna ("**Titolare**");

e

(ii) la **Società "_____"**, rappresentata da ….., in qualità di …… (di seguito indicato "**Responsabile**"), quale mandataria del Raggruppamento Temporaneo di Imprese costituito con atto Rep. n. _____ del _____, tra _____,

singolarmente denominati "**Parte**" e congiuntamente "**Parti**",

PREMESSO CHE:

1. ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 del Consiglio e del Parlamento europeo del 27 aprile 2016 sulla protezione e la libertà di circolazione dei dati personali delle persone fisiche ("**GDPR**"), il Responsabile nominato per mezzo del presente accordo è competente esclusivamente per il trattamento dei dati personali nell'ambito del "Contratto d'appalto _____", stipulato tra il Titolare e la società _____ in data _____, rep. n. _____ (il "**Contratto**");

2. in virtù del suindicato Contratto, il Responsabile si assume l'obbligo di fornire al Titolare i servizi di cui all'Allegato 1 del presente ADP (i "**Servizi")**;

3. la prestazione dei Servizi può di volta in volta comportare l'accesso del Responsabile o la comunicazione a quest'ultimo di informazioni del Titolare configurabili quali dati personali ai sensi del GDPR e da ulteriori disposizioni e leggi applicabili in materia di protezione dei dati;

4. le Parti convengono che i trasferimenti dei dati disciplinati dal presente ADP rientrano nell'ambito di applicazione dell'articolo 28 del GDPR e che il Responsabile si qualifica quale responsabile del trattamento ai sensi del GDPR; inoltre, è intenzione delle Parti utilizzare l'ADP quale accordo contrattuale per disciplinare il trattamento dei dati.

CIÒ PREMESSO, al fine di prestare garanzie sufficienti alla tutela della vita privata, delle libertà e dei diritti fondamentali delle persone fisiche circa il trasferimento dal Titolare al Responsabile dei dati personali di cui all'Allegato 1, le Parti convengono quanto segue:

1. Definizioni

Ai fini del presente ADP, trovano applicazione la terminologia e le definizioni utilizzate nel GDPR, nonché tutti i termini definiti qui di seguito.

"Violazione della sicurezza":	si intende una violazione della sicurezza che comporta, incidentalmente o illecitamente, la distruzione, perdita, modifica, comunicazione non autorizzata o l'accesso a dati personali trasmessi, memorizzati o altrimenti trattati che interessano i dati personali del

Titolare disciplinati dal DPA.

"Sub-responsabile": si intende qualunque ulteriore responsabile, stabilito all'interno o al di fuori dell'UE/SEE, nominato dal Responsabile quale sub-fornitore del Titolare per la prestazione dei Servizi o di parte di essi, a condizione che tale Sub-responsabile abbia accesso ai dati personali del Titolare esclusivamente allo scopo di eseguire i Servizi subappaltati per conto del Titolare.

2. Obblighi generali delle Parti

2.1 Obblighi del Titolare

2.1.1 Il Titolare è tenuto a confermare che le attività di trattamento dei dati personali, come descritte nel Contratto e nel presente ADP, siano lecite, eque e trasparenti in relazione ai soggetti interessati, di cui all'Allegato 1.

2.1.2 Il Titolare è tenuto a confermare prima delle operazioni di trattamento, che le misure tecniche e organizzative di cui all'Allegato 2 implementate dal Responsabile siano adeguate e atte a proteggere i diritti dei soggetti interessati.

2.2 Obblighi del Responsabile

2.2.1 Il Responsabile dichiara e garantisce che tratterà i dati personali esclusivamente per conto del Titolare e secondo le istruzioni impartite dal Titolare e contenute nel presente ADP, nonché di informare senza indebito ritardo il Titolare qualora non sia in grado, per qualunque ragione, di ottemperare a tali disposizioni; nel qual caso il Titolare potrà sospendere il trasferimento dei dati e/o risolvere il presente ADP.

2.2.3 Il Responsabile è tenuto ad implementare le misure tecniche ed organizzative di cui all'Allegato 2 prima di procedere al trattamento dei dati personali per conto del Titolare. Il Responsabile può di volta in volta modificare le misure tecniche ed organizzative a condizione che le nuove misure non siano meno stringenti rispetto a quelle di cui all'Allegato 2 e che le stesse siano state previamente notificate al Titolare.

2.2.4 Il Responsabile dichiara e garantisce che risponderà prontamente ed adeguatamente a tutte le richieste del Titolare relative al trattamento dei dati personali soggetti a trasferimento e di conformarsi al parere emesso dall'autorità di controllo sul trattamento dei dati trasferiti.

2.2.5 Il Responsabile ha l'obbligo di garantire che le persone autorizzate al trattamento dei dati personali per conto del Titolare, in particolare i dipendenti del Responsabile ed eventuali Sub-responsabili compresi i loro dipendenti, tratteranno tali dati personali secondo le istruzioni impartite dal Titolare.

2.2.6 Il Responsabile è tenuto a fornire al Titolare informazioni sulle attività di trattamento riguardanti i servizi disciplinati dall'ADP, nella misura necessaria al Titolare per l'adempimento dell'obbligo di mantenere il registro del trattamento.

2.2.7 Su richiesta del Titolare, il Responsabile è tenuto a coadiuvarlo al fine di effettuare la valutazione d'impatto sulla protezione dei dati, nonché la consultazione preventiva con le autorità di controllo, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile.

2.2.8 Se il Responsabile nomina un DPO (ove previsto dalla legge applicabile in materia di protezione dei dati), questi sarà tenuto a comunicare i dettagli di contatto del DPO al Titolare.

2.2.9 Al termine della prestazione dei Servizi, il Responsabile è tenuto, su richiesta del Titolare, a cancellare o restituire al Titolare tutti i dati personali (e qualsiasi copia esistente) trattati dal Responsabile per conto del Titolare di cui al presente ADP. La cancellazione dei dati personali da parte del Responsabile dovrà essere certificata al Titolare, conformemente alla normativa vigente in materia di conservazione dei dati personali. In questo caso, il Responsabile si impegna a garantire la riservatezza dei dati personali trasferiti e di non trattare di propria iniziativa tali dati.

2.3 Le Parti sono tenute ad osservare le previsioni normative del GDPR e di qualsiasi altra legge in materia di protezione dei dati che trovano applicazione nei confronti del Titolare nella sua qualità di titolare del trattamento e al Responsabile nella sua qualità di responsabile del trattamento.

3. Istruzioni

3.1 Ai sensi della sezione 2.2.1 dell'ADP, il Responsabile si obbliga a trattare i dati personali esclusivamente per conto del Titolare e in conformità alle istruzioni impartite dal Titolare, anche per quanto concerne i trasferimenti dei dati personali a un Paese terzo o ad un'organizzazione internazionale, fermo restando quanto previsto dalla normativa vigente a cui il Responsabile è soggetto. In tale caso, se il Responsabile non si limita a trattare i dati personali in conformità alle istruzioni impartite dal Titolare, egli sarà tenuto a dare previa comunicazione al Titolare di quanto previsto dalla normativa vigente, a meno che la previsione normativa in questione ne vieti la comunicazione per ragioni di interesse pubblico rilevante. In tale circostanza, le informazioni da comunicare al Titolare dovranno riportare quanto previsto normativa vigente.

3.2 Il Titolare può fornire specifiche alle istruzioni riportate nel presente ADP e nel Contratto, nonché ulteriori istruzioni. Qualsiasi ulteriore istruzione che esula da quelle riportate nell'ADP o nel Contratto necessiterà di una richiesta di modifica ai sensi del Contratto.

3.3 Le istruzioni sono fornite per iscritto, a meno che l'urgenza o altre circostanze del caso richiedano una forma diversa.

3.4 Oltre agli obblighi di comunicazione previsti dall'ADP, il Responsabile è tenuto a comunicare immediatamente al Titolare eventuali istruzioni che ritiene siano in violazione di leggi applicabili in materia di protezione dei dati ("**Istruzione Contestata**"). A seguito di tale comunicazione il Responsabile non sarà tenuto ad osservare l'Istruzione Contestata. Se, a seguito delle informazioni fornite dal Responsabile, il Titolare conferma l'Istruzione Contestata e riconosce la propria responsabilità, il Responsabile sarà tenuto ad osservare l'Istruzione Contestata a meno che questa sia collegata (i) all'implementazione di misure tecniche e organizzative; (ii) ai diritti dei soggetti interessati; o (iii) alla nomina di sub-responsabili. Nei suddetti casi, il Titolare può contattare l'autorità di controllo competente per una valutazione legale dell'Istruzione Contestata. Se l'autorità di controllo conferma la legittimità dell'Istruzione Contestata, il Responsabile sarà tenuto ad osservarla.

4. Monitoraggio, audit e ispezioni da parte del Titolare

4.1 Il Responsabile è tenuto a monitorare, tramite strumenti adeguati, la propria conformità, nonché quella dei propri dipendenti e sub-responsabili rispetto agli obblighi in materia di protezione dei dati previsti nell'ADP e di cui all'articolo 28 del GDPR. Il Responsabile deve mettere a disposizione del Titolare qualsiasi

informazione atta a dimostrare l'osservanza di tali obblighi. Per documentare l'attività di auto-monitoraggio, il Responsabile è tenuto a fornire al Titolare periodicamente (almeno annualmente) e, se disponibili, apposite relazioni ad hoc (anche su richiesta del Titolare) su tali controlli ("**Relazioni di Audit**"). Le Relazioni di Audit devono contenere informazioni relative ai Servizi ed i sistemi di trattamento dati, conferma delle istruzioni fornite a dipendenti e Sub-responsabili, osservanza delle misure tecniche ed organizzative, conferma dell'impegno a rispettare la riservatezza, l'indicazione di eventuali violazioni dei dati personali (data breaches) e/o incidenti che potrebbero minarne la sicurezza, ed i miglioramenti necessari e/o richiesti. Il Titolare ha il diritto di richiedere le relazioni di audit in qualsiasi momento in modo da controllare l'ottemperanza del Responsabile ai propri obblighi in materia di protezione dei dati.

4.2 Il Titolare può richiedere di svolgere direttamente le ispezioni o affidarle ad un revisore terzo ("**Audit in loco**"). L'Audit in loco è soggetto alle seguenti condizioni: (i) deve riguardare solamente il personale e le strutture di trattamento del Responsabile coinvolte nelle attività di trattamento di cui al DPA; (ii) deve essere svolto non più di una volta l'anno o secondo quanto previsto dalla legge applicabile in materia di protezione dei dati o dall'autorità di controllo competente o immediatamente successive al verificarsi di una Violazione dei Dati (Data Breach) che incide sui dati personali trattati dal Responsabile di cui al presente ADP; (iii) deve prevedere un congruo preavviso e può essere svolto durante il normale orario di lavoro, senza interrompere la continuità delle attività commerciali del Responsabile e in ottemperanza alle politiche sulla sicurezza del Responsabile; e (iv) il Titolare si fa carico di tutte le spese derivanti o in relazione agli Audit in loco presso il Titolare o il Responsabile, a meno che tali Audit in loco rivelano che il Responsabile non agisce in conformità agli obblighi previsti dall'articolo 28 del GDPR, il DPA o qualsiasi altra legge applicabile in materia di protezione dei dati, nel qual caso tutte le spese saranno a carico del Responsabile. Il Titolare può predisporre una relazione di audit che riassume i risultati e le osservazioni emerse dagli Audit in loco ("**Relazione di audit in loco**"). Le Relazioni di audit in loco e le Relazioni di Audit sono informazioni riservate del Responsabile e il Titolare si impegna a non divulgarle a terzi, ad eccezione che ai propri consulenti anche in materia legale, al proprio funzionario preposto alla protezione dei dati (DPO), ai propri dipendenti e società affiliate, e fatto salvo se è comunque tenuto a divulgarne il contenuto ai sensi della legge applicabile in materia di protezione dei dati, o su richiesta dell'autorità di controllo competente o se il Responsabile presta il consenso alla divulgazione.

5. Riservatezza dei dati

5.1 Il Responsabile è tenuto ad assicurarsi che le persone autorizzate a trattare i dati personali per conto del Titolare, in particolare i propri dipendenti, eventuali sub-responsabili e i relativi dipendenti si impegnino a rispettarne la riservatezza o siano soggetti ad un obbligo legale di riservatezza dei dati personali e delle operazioni di trattamento di cui al presente ADP. Su richiesta del Titolare, il Responsabile è tenuto a dimostrare la conformità a tale obbligo.

6. Obblighi di comunicazione e violazione della sicurezza

6.1 Oltre agli obblighi di comunicazione previsti dal presente ADP, il Responsabile è tenuto a notificare al Titolare senza indebito ritardo: (i) qualsiasi richiesta legalmente vincolante di comunicazione di dati personali presentata da autorità giudiziarie o di polizia, salvo che la comunicazione non sia vietata da norme specifiche (ad esempio da norme di diritto penale miranti a tutelare il segreto delle indagini), o da eventuali ordinanze del tribunale e di autorità/enti regolatori competenti relativi al trattamento di dati personali previsti dal DPA; (ii) eventuali reclami o richieste da parte di soggetti interessati (e.g. in materia di accesso, rettifica, cancellazione, limitazione di trattamento, portabilità dei dati, opposizione al trattamento dei dati, decisioni automatizzate) senza dover rispondere a tale richiesta a meno che il Responsabile sia stato altrimenti autorizzato o secondo

quanto altrimenti previsto da leggi applicabili; e (iii) eventuali Violazioni della Sicurezza come definito nel presente ADP o dalla legge applicabile in materia di protezione dei dati relativi ai Servizi forniti dal Responsabile.

6.2 In caso di Violazione della Sicurezza, il Responsabile deve darne comunicazione al Titolare entro un massimo di 4 (quattro) ore da quando si è verificata. Entro le successive 20 (venti) ore il Responsabile deve altresì raccogliere e fornire al Titolare le seguenti informazioni di dettaglio:

a) il tipo di violazione [1];
b) la natura, la sensibilità e il volume dei dati personali interessati;
c) la facilità di identificazione delle persone;
d) la gravità delle conseguenze per gli interessati (ad esempio: danni fisici, disagio psicologico, umiliazione o danni alla reputazione);
e) l'elenco delle persone interessate dalla violazione di sicurezza (se disponibili), incluse le informazioni di contatto;
f) le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di record di dati personali interessati;
g) le probabili conseguenze, per il Titolare, della violazione dei dati personali subita dal Responsabile e/o dai Sub-responsabili;
h) le misure adottate o da adottare per affrontare la violazione dei dati personali, per attenuare gli effetti e ridurre al minimo i danni derivanti dalla violazione della sicurezza.

6.3 Il Responsabile, ai sensi della legge applicabile sulla protezione dei dati personali, in caso di Violazione della Sicurezza, dovrà assistere il Titolare nell'obbligo di informare l'Autorità di controllo e gli interessati, laddove necessario, fornendo le informazioni a sua disposizione di cui al punto precedente e tenendo conto della natura del trattamento.

6.4 Il Responsabile sarà tenuto a risarcire e tenere indenne il Titolare da qualsiasi reclamo, perdita, responsabilità, valutazione, danno, costo, sanzione amministrativa e altra spesa (incluse le spese legali) derivante o risultante da qualsiasi rivendicazione, richiesta, istanza, azione o altre procedura di terzi (comprese le autorità di controllo) subite dal Titolare a seguito di una Violazione della Sicurezza causato dal Responsabile, dai dipendenti, amministratori, dirigenti, agenti e altri collaboratori del Responsabile, o dal Sub-responsabile del Responsabile.

7. Risposte alle richieste di soggetti interessati

7.1 Il Responsabile coadiuverà il Titolare, soprattutto tramite l'attuazione di adeguate misure tecniche ed organizzative, per quanto più possibile, nell'adempimento dell'obbligo del Titolare di rispondere alle richieste di soggetti interessati circa l'esercizio dei propri diritti.

7.2 Oltre a quanto sopra descritto, il Titolare può richiedere al Responsabile di coadiuvarlo al fine di rispondere alle richieste di soggetti interessati circa l'esercizio dei propri diritti. Il Titolare è tenuto a stabilire se un soggetto interessato ha il diritto o meno di esercitare tali diritti e di fornire ulteriori istruzioni al Responsabile circa l'assistenza necessaria.

[1] Tipi di violazioni dei dati personali:

- "Violazione della riservatezza" - in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
- "Violazione della disponibilità" - in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali.
- "Violazione dell'integrità": in caso di alterazione non autorizzata o accidentale dei dati personali.

Esempi di perdita di disponibilità si hanno nei casi in cui i dati sono stati cancellati accidentalmente o da una persona non autorizzata oppure, in caso di dati criptati, quando si perde la chiave di decifratura. Nel caso in cui il Titolare non possa ripristinare l'accesso ai dati, ad esempio tramite un backup, ciò viene considerato come una perdita permanente di disponibilità.

8. Sub-trattamento

8.1 Il Responsabile non instaurerà alcun rapporto contrattuale con Sub-responsabili senza averne prima informato il Titolare e ottenuto il previo consenso scritto. Qualora il Responsabile ottenga tale previa autorizzazione, la nomina di eventuali Sub-responsabili è soggetta alle seguenti condizioni:

(a) Il Responsabile è tenuto a scegliere diligentemente il Sub-responsabile prestando particolare attenzione alla reputazione e l'esperienza nel fornire i Servizi subappaltati nonché l'adeguatezza delle misure tecniche e organizzative. Il Responsabile è tenuto a stipulare un accordo scritto con qualsiasi eventuale Sub-responsabile il quale deve (i) prevedere nei confronti del Sub-responsabile gli stessi obblighi previsti dal DPA al Responsabile, nella misura applicabile ai Servizi subappaltati, (ii) descrivere i Servizi subappaltati, e (iii) le misure tecniche e organizzative che il Sub-responsabile è tenuto ad implementare di cui all'Allegato 2 dell'ADP, laddove applicabili ai Servizi subappaltati. Il Responsabile è tenuto a trasmettere tempestivamente al Titolare copia del contratto stipulato tra il Responsabile e il Sub-responsabile.

(b) Il Responsabile, per tutta la durata del presente ADP e senza alcun onere a carico del Titolare, è tenuto a monitorare attivamente, verificare regolarmente e, laddove applicabile, adottare le misure atte a garantire la conformità da parte di ciascun Sub-responsabile dei propri obblighi, riferire tempestivamente al Titolare qualsiasi mancata conformità individuata o segnalata dal Sub-responsabile e tutte le misure adottate per porre rimedio ai casi di non conformità riscontrati. Qualora in qualsiasi momento un Sub-responsabile non sia in grado di porre rimedio ad una situazione di non conformità entro un termine ragionevole dalla comunicazione che chiede di porvi rimedio, il Titolare potrà revocare l'autorizzazione concessa per la nomina del Sub-responsabile. Qualora il Sub-responsabile non adempia ai propri obblighi in materia di protezione dei dati, il Responsabile rimane pienamente responsabile nei confronti del Titolare per l'inadempimento da parte del Sub-responsabile dei suoi obblighi in materia di protezione dei dati.

(c) Il Responsabile è tenuto ad informare il Titolare almeno 30 (trenta) giorni prima del conferimento al Sub-responsabile (nominato in conformità con il presente ADP) dell'accesso ai dati personali trattati nell'ambito dell'ADP stesso, in maniera da consentire al Titolare di opporsi alla nomina del Sub-responsabile.

(d) In presenza di motivi legittimi, il Titolare potrà chiedere al Responsabile di revocare in ogni momento la nomina di qualsiasi Sub-responsabile. In tale caso si applicherà *mutatis mutandis* la sezione 8 (c) del presente ADP.

(e) Se il Sub-responsabile è stabilito in un paese al di fuori dell'UE/SEE che non fornisce un adeguato livello di protezione dei dati personali, il Responsabile sarà tenuto a (i) garantire che il Titolare e il Sub-responsabile stipulino un accordo per il trattamento dei dati basato sulle clausole contrattuali standard per il trasferimento dei dati personali a Responsabili stabiliti in paesi terzi ai sensi della decisione della Commissione 2010/87/EU del 5 febbraio 2010, o (ii) dovrà comunicare al Titolare informazioni sulla certificazione al programma di Privacy Shield del Sub-responsabile e regolarmente, almeno annualmente, confermare che la certificazione al programma di Privacy Shield del Sub-responsabile sia valida, o (iii) fornire al Titolare ulteriori informazioni e documenti relativi al meccanismo per il trasferimento internazionale dei dati ai sensi dell'articolo 46 del GDPR impiegato per la comunicazione legittima dei dati personali dal Titolare al Sub-responsabile.

9. Efficacia, durata e termine

9.1 L'efficacia del presente ADP decorre dal _____ ed ha la medesima durata prevista dal Contratto. Fatto salvo quanto stabilito nell'ADP, le condizioni e i diritti di recesso sono gli stessi previsti nel Contratto.

10. Prevalenza tra contratti e clausola di esonero

10.1 Qualora vi siano contraddizioni o incompatibilità tra le clausole del presente ADP e il Contratto e/o altri contratti stipulati tra le Parti, prevarranno le clausole del presente ADP che disciplinano gli obblighi delle Parti in materia di protezione dei dati. Il presente ADP prevale anche nell'ipotesi in cui vi siano dubbi se le clausole contrattuali contenute in tali ulteriori accordi disciplinano gli obblighi delle Parti in materia di protezione dei dati.

10.2 Il presente ADP non comporta l'insorgere, a carico del Titolare, di alcun onere, di qualsiasi natura, ulteriore ed aggiuntivo rispetto a quelli espressamente previsti e pattuiti nel Contratto.

11. Miscellanea

11.1 Ciascuna Parte è responsabile per l'adempimento dei propri obblighi previsti dal presente ADP e dalla normativa vigente applicabile in materia di protezione dei dati. Eventuali responsabilità derivanti o in connessione ad un inadempimento degli obblighi in materia di protezione dei dati viene disciplinata dalle disposizioni in materia di responsabilità stabilite o altrimenti applicabili al Contratto, fermo restando quanto previsto nel presente ADP. Se in materia di responsabilità trovano applicazione le disposizioni contrattuali previste o altrimenti applicabili al Contratto, al fine del calcolo del limite di responsabilità e/o per determinare l'applicazione di ulteriori limiti alla responsabilità, si applicherà quanto previsto nel Contratto e non nel presente ADP.

11.2 Il Responsabile si impegna a tutelare, manlevare e tenere indenne il Titolare, i suoi collaboratori, amministratori, dipendenti, successori e agenti (collettivamente le "**Parti indennizzate**") da qualsiasi azione, danno, responsabilità, valutazione, perdita, costo, sanzione amministrativa e altra spesa (ivi comprese ragionevoli onorari e spese legali) derivanti da qualsiasi azione legale, pretesa, richiesta, ordine o altro procedimento da parte di terzi (incluse le autorità di controllo) che derivano da o riguardano la violazione degli obblighi del Titolare di cui al presente ADP.

11.3 Il foro competente per qualsiasi eventuale controversia relativa al presente ADP viene stabilito dall'articolo 19 del Contratto.

11.4 L'inapplicabilità o l'invalidità di una o più disposizioni del presente ADP non pregiudica le restanti parti dell'Accordo. La disposizione invalida o inapplicabile potrà all'occorrenza essere (i) modificata al fine di garantirne validità ed opponibilità, rispettando il più fedelmente possibile l'intenzione delle Parti o – qualora questo non sia possibile – (ii) interpretata come se la stessa non fosse mai stata parte del presente ADP. Quanto precede si applica anche nel caso in cui l'Accordo presenti lacune.

Firme per il Titolare
Autorità di sistema portuale del Mare di Sardegna,
Nome: Massimo Deiana
Titolo: Presidente dell'Autorità di Sistema Portuale del Mare di Sardegna

Data: _____

Firma:

_____

Firma per il Responsabile del trattamento dei dati
_____ [Firmato da _____]
Nome:
Titolo:

Data: _____

Firma:

_____

ALLEGATO 1

Il Data Protection Officer del Titolare
La seguente persona è stata nominata Data Protection Officer del Titolare:

Alessandro Franchi
Autorità di sistema portuale del Mare di Sardegna

Data Protection Office
Sede: Molo Dogana – 09123 Cagliari - Italia
Indirizzo PEC: adsp@pec.adspmaredisardegna.it
Indirizzo Email: franchi@adspmaredisardegna.it
Il Responsabile riceverà immediata comunicazione di eventuali cambi di nomina del Data Protection Officer e di eventuali cambi dei suddetti contatti.

Il Data Protection Officer del Responsabile
La seguente persona è stata nominata Data Protection Officer del Responsabile:

_____
_____

Data Protection Office:
Sede: _____
Indirizzo PEC: _____
Indirizzo Email: ____@_____
Il Titolare riceverà immediata comunicazione di eventuali cambi di nomina del Data Protection Officer e di eventuali cambi dei suddetti contatti.

Soggetti Interessati
I dati personali trattati riguardano le seguenti categorie di soggetti interessati:

- ☐ Avventori
- ☐ Candidati
- ☐ Clienti
- ☐ Collaboratori
- ☐ Utenti
- ☐ Dipendenti
- ☐ Consiglieri
- ☐ Fornitori
- ☐ Altro (specificare

Categorie di dati
I dati personali trattati riguardano le seguenti categorie di dati:

- ☐ Dati Comportamentali
- ☐ Dati Comuni
- ☐ Dati Particolari
- ☐ Dati identificativi

- ☐ Dati videosorveglianza (immagini)
- ☐ Dati Economici
- ☐ Dati giudiziari

Categorie speciali di dati (se del caso)
I dati personali trattati riguardano le seguenti categorie speciali di dati
Non è previsto il trattamento di dati sensibili.

Operazioni di trattamento
I dati personali trattati rientrano nelle seguenti attività base di trattamento:

- **Oggetto del trattamento:** la raccolta, riorganizzazione, elaborazione e cancellazione dei dati per la gestione dei processi portuali.

- **Natura e finalità del trattamento:** La natura e finalità del trattamento è in funzione dell'attività di sicurezza all'interno dell'ambito portuale.

ALLEGATO 2

Descrizione delle misure tecniche e organizzative di sicurezza implementate dal Responsabile (e dai suoi Sub-responsabili):

AREE DI SICUREZZA	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI
NETWORK E SISTEMI DI SICUREZZA	Firewall e router saranno configurati al fine di limitare il traffico, in entrata e in uscita, da reti "non attendibili" (inclusi wireless) ed i sistemi. Tutto il resto del traffico ad eccezione dei protocolli necessari all'ambiente che tratta dati personali sarà negato.
	I firewall dell'applicazione saranno configurati davanti ai server Web appartenenti all'ambiente che tratta dati personali, al fine di verificare e convalidare il traffico che è diretto al server. Qualsiasi servizio o traffico non autorizzato sarà bloccato e dovrà essere generato un avviso.
SICUREZZA DEI DATI	I supporti (rimovibili e non rimovibili) contenenti dati personali saranno protetti contro l'accesso non autorizzato attraverso misure di sicurezza fisica (ad es. conservandolo in un luogo sicuro chiuso a chiave) e logica (ad es. controllo degli accessi, ecc.).
	Per la dismissione degli asset ICT saranno messe in atto procedure di pulizia sicura al fine di rimuovere tutti i dati personali e/o sovrascrivere in modo sicuro prima dello smaltimento o del riutilizzo.
	I documenti cartacei e i supporti magnetici/ottici (ad es. dischi rigidi, DVD, CD, smart card, chiavette USB) saranno distrutti o resi inutilizzabili per garantire che i dati e le informazioni in essi contenuti non potranno essere ricostruiti e/o utilizzati (anche parzialmente) da terze parti non autorizzate. I documenti cartacei saranno fisicamente distrutti prima di essere cestinati attraverso dispositivi specifici quali distruggi documenti.
	I dipendenti saranno adeguatamente istruiti e formati sulle corrette regole di condotta da adottare per la protezione dei dati personali contenuti nei documenti cartacei (ad es: in caso di allontanamento dalla postazione di lavoro assicurarsi che nessuno possa accedere alle informazioni riservate, proteggere i documenti originali e le fotocopie da furto o uso non autorizzato, conservare la documentazione in cassetti e armadi chiusi alla fine della sessione di lavoro).
DISPONIBILITÀ DEI DATI	Saranno messe in atto procedure adeguate per ripristinare la disponibilità dei dati personali (come diritto dell'interessato) in modo tempestivo. Le procedure di backup garantiranno copie dei dati personali almeno settimanalmente.
IDENTITY AND ACCESS MANAGEMENT	L'autorizzazione ad accedere agli ambienti di produzione contenenti dati personali saraà fornita secondo i principi del "need to know" e del "least privilege".
	Saranno implementate policy e le procedure per garantire la corretta identificazione degli utenti e degli amministratori che accedono alle componenti di sistema che gestiscono i dati personali. A tutti gli utenti saranno assegnati un nome utente univoco prima di consentire loro di accedere ai sistemi di autenticazione e ai dati personali.
	Gli accessi amministrativi remoti individuali ai sistemi che gestiscono i dati personali saranno protetti mediante un meccanismo di autenticazione che richiede modifica della password ogni 90 giorni. Inoltre, si consiglierà di dotarsi di strumenti per la gestione delle password (tool ad hoc) per garantire la sicurezza delle credenziali.

AREE DI SICUREZZA	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI
	Le password per i sistemi e i dispositivi che gestiscono dati personali saranno impostate in modo da contenere almeno 8 cifre non facilmente attribuibili all'utente e saranno modificate almeno ogni 3 mesi.
	Le risorse di sistema e il diritto di accesso saranno assegnati in modo univoco ad ogni user account.
	Tutti gli accessi ai database contenenti dati personali saranno protetti / controllati come segue: ▪ le credenziali dell'applicazione per accedere ai database non potranno essere utilizzate dai singoli utenti o da altri processi non applicativi; ▪ tali credenziali saranno adeguatamente protette da potenziali abusi; ▪ l'accesso sarà concesso solo al personale che ne ha realmente bisogno per l'esecuzione del proprio lavoro / dei propri compiti; ▪ sarà implementata una procedura formale di registrazione e de-registrazione degli utenti per consentire l'assegnazione dei diritti di accesso per la gestione dei dati personali.
	La visibilità dei dati personali sarà limitata al solo set di informazioni necessario per le singole attività di elaborazione. Non saranno messi a disposizione degli utenti dati personali non necessari.
	I diritti di accesso ai dati personali degli utenti saranno rivisti / ricertificati a intervalli regolari e, in ogni caso, almeno una volta all'anno, secondo il corretto processo di Identity and Access Management.
	Agli amministratori sarà richiesto di accedere a un sistema utilizzando un account non amministrativo e soggetto a tracciatura di tutte le attività. Pertanto, una volta effettuato l'accesso alla macchina, l'amministratore otterrà i privilegi amministrativi.
***LOGGING* E MONITORAGGIO**	Saranno registrate almeno le seguenti voci del registro di controllo per tutti i componenti del sistema che elaborano i dati personali per ciascun evento: - Identificazione dell'utente - Tipo di evento - Data e ora - Indicazione di successo o fallimento - Fonte dell'evento - Identità dei dati interessati (NDG per i clienti e ID per gli altri), dei componenti di sistema o risorse.
	In caso di necessità e/o di esigenza normativa, il Titolare del trattamento dei dati personali avrà il diritto di ottenere i log dai Responsabili del trattamento e/o dai Sub-responsabili.
ORGANIZZAZIONE E SICUREZZA DELLE PERSONE	Saranno messe in atto procedure adeguate per garantire la disponibilità continua di dati personali; il personale di back up sarà identificato per garantire la continuità del servizio all'interessato che desidera accedere ai propri dati personali.
	Sarà attuato un programma formale di sensibilizzazione sulla sicurezza per rendere consapevole tutto il personale delle politiche e procedure relative alla sicurezza dei dati personali. Saranno eseguiti test periodici o simulazioni per valutare se i dipendenti fanno clic su un collegamento contenuto in email sospette o forniscono informazioni personali / sensibili senza seguire procedure di sicurezza appropriate per verificare l'affidabilità della fonte. Di conseguenza, sarà fornita una formazione mirata a quei dipendenti che sono vittima del test.
	Saranno stipulati chiari accordi contrattuali con i fornitori dei servizi, al fine di pattuire la loro responsabilità in merito alla sicurezza dei dati personali che elaborano / memorizzano / trasmettono per conto del Titolare.

AREE DI SICUREZZA	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI
	Le responsabilità e i doveri dei dipendenti relative alla riservatezza dei dati personali saranno chiaramente esplicitate come valevoli anche dopo la cessazione o il cambio di impiego.
DATA PROTECTION BY DESIGN	I processi e gli strumenti per il Secure Software Development Lifecycle (SDLC) saranno integrati con controlli e requisiti di sicurezza appropriati, al fine di garantire che i nuovi software/applicazioni ICT siano progettati e sviluppati tenendo in considerazione i requisiti della sicurezza integrata.
	I processi di gestione delle modifiche ICT saranno integrati con controlli e requisiti di sicurezza appropriati, al fine di garantire la protezione continua del software / applicazioni ICT in vigore subito dopo modifiche rilevanti.
VIOLAZIONE DEI DATI PERSONALI	I processi e gli strumenti per la gestione degli incidenti saranno correttamente implementati e/o migliorati al fine di consentire il rilevamento e la classificazione delle violazioni dei dati personali in modo che siano correttamente comunicati al Titolare affinché possa provvedere entro i termini stabiliti nel paragrafo "Obblighi di comunicazione e Violazione di Sicurezza".
	Sarà creato e mantenuto aggiornato uno specifico registro delle violazioni dei dati personali.

ANNO MMXXIII

Autorità di Sistema Portuale
del Mare di Sardegna

Porti di: Cagliari | Olbia | Porto Torres | Oristano | Golfo Aranci | Portovesme | Santa Teresa Gallura | Arbatax

AUTORITÀ DI SITEMA PORTUALE DEL MARE DI SARDEGNA

COOKIES
E ALTRI STRUMENTI DI TRACCIAMENTO

ADDENDUM ALLE LINEE GUIDA PER IL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLO SVOLGIMENTO DELLE ATTIVITÀ ISTITUZIONALI DELL'AUTORITÀ DI SISTEMA PORTUALE DEL MARE DI SARDEGNA

Sommario

Introduzione. Fonti normative.

Le presenti Linee guida traducono indicazioni operative relative all'utilizzo (scrittura e lettura) di cookies e di altri strumenti di tracciamento all'interno del terminale di un utente (visitatore del sito) e alla fornitura della relativa informativa.

Le fonti normative di riferimento sono:

- Direttiva 2002/58/CE (c.d. direttiva ePrivacy) e successive modifiche, come recepita nell'ordinamento nazionale all'art. 122 del d.lgs. 30 giugno 2003, n. 196;
- Regolamento per la protezione dei dati personali (UE) n. 675/2016 (GDPR), per ciò che concerne specificamente la nozione di consenso di cui agli artt. 4, punto 11) e 7 e al considerando 32, come da ultimo interpretati dalle Linee Guida del WP29 adottate il 10 aprile 2018, ratificate dal Comitato europeo per la Protezione dei dati personali (di seguito, EDPB) il 25 maggio 2018 e sostituite, da ultimo, dalle *Guidelines 05/2020 on consent under Regulation* 2016/679 adottate il 4 maggio 2020.

Si noti che ogniqualvolta la direttiva renda più specifiche le prescrizioni del Regolamento, essa, in quanto dotata di specialità, dovrà prevalere sulle - più generali - disposizioni del GDPR.

Inoltre, la direttiva ePrivacy non contempla ulteriori basi giuridiche che rendano legittimo il trattamento se non in presenza del consenso dell'interessato. In nessun caso sarà pertanto possibile invocare ad esempio, la scriminante del legittimo interesse del titolare per giustificare il ricorso a cookies o altri strumenti di tracciamento.

ANNOTAZIONE:

Sebbene la direttiva ePrivacy preveda in alcuni casi l'obbligo di acquisizione del consenso all'impiego di cookie e altri strumenti di tracciamento, è nel GDPR che andranno ricercate le specifiche caratteristiche di quel consenso ai fini della sua validità e conformità alla disciplina generale.

1. Tipologie di cookies.

Per una corretta gestione dei cookies e degli altri identificatori, occorre distinguere due macrocategorie:

- **tecnici**, utilizzati al solo fine di consentire la navigazione sul sito;
- **di profilazione**, utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti in modo che sia possibile al Titolare, tra l'altro, modulare la fornitura del servizio in modo sempre più personalizzato al di là di quanto strettamente necessario all'erogazione del servizio, nonché inviare messaggi pubblicitari mirati.

Per l'utilizzo di **cookies tecnici**, il Titolare del trattamento deve fornire specifica informativa, anche eventualmente inserita all'interno di quella di carattere generale, rientrando il loro impiego in una ipotesi codificata di esenzione dall'obbligo di acquisizione del consenso dell'interessato.

I cookies e gli altri strumenti di tracciamento per **finalità di profilazione**, invece, possono essere utilizzati esclusivamente previa acquisizione del consenso del contraente o utente.

Affinché i cookie di profilazione siano equiparati ai tecnici è indispensabile precludere la possibilità che si pervenga, mediante il loro utilizzo, alla diretta individuazione dell'Interessato (cd. *single out*), il che equivale a impedire l'impiego di cookies di profilazione che, per le loro caratteristiche, possano risultare identificatori diretti ed univoci. La struttura del cookie di profilazione dovrà allora prevedere la possibilità che lo stesso cookie sia riferibile non soltanto ad uno, bensì a più dispositivi, in modo da creare una ragionevole incertezza sull'identità informatica del soggetto che lo riceve. Di regola questo effetto si ottiene mascherando opportune porzioni dell'indirizzo IP all'interno del cookie.

2. La gestione del consenso.

Per quanto riguarda il consenso, è utile ricordare che esso deve essere espresso in modo inequivocabile, non condizionato, a seguito di adeguata informazione e per mezzo di un "atto positivo".

Campi pre-selezionati con il consenso non rendono il consenso valido.

Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, mentre non configurano consenso il silenzio, l'inattività o la preselezione di caselle.

Il consenso, inoltre, deve essere necessariamente:

- **revocabile**
- **sempre revocabile**
- **facilmente revocabile.**

Il consenso deve essere richiesto, qualora il trattamento abbia più finalità, specificamente per ognuna di esse.

La richiesta deve essere chiara, concisa e non interferire immotivatamente con la navigazione; pertanto, il semplice *scrolling* non è mai idoneo, di per sé, ad esprimere compiutamente la manifestazione di volontà dell'Interessato volta ad accettare cookies diversi da quelli tecnici.

Con riferimento al cd. *cookie wall*, ossia quel meccanismo vincolante (cd. *"take it or leave it"*), col quale l'utente venga obbligato ad esprimere il proprio consenso alla ricezione di cookies (ovvero altri strumenti di tracciamento), pena l'impossibilità di accedere al sito, tale meccanismo, non conforme alle caratteristiche imposte dal GDPR con particolare riferimento al requisito della "libertà" del consenso, è da ritenersi illecito.

3. Il banner.

Affinché il banner sia conforme al GDPR, l'utente, accedendo per la prima volta alla home page (o ad altra pagina) del sito web, deve visualizzare immediatamente un'area delimitata (o banner, appunto) le cui dimensioni siano tali da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che sta visitando, ma che altresì evitino il rischio che l'utente possa far ricorso inavvertitamente a comandi e dunque compiere scelte indesiderate o inconsapevoli.

Non è conforme al GDPR **l'eccessiva riproposizione del banner** ai fini dell'acquisizione del consenso laddove l'utente l'abbia già in precedenza negato il consenso, poiché una reiterazione potrebbe condizionarne la libertà di scelta inducendolo ad accettare pur di proseguire nella navigazione libero dalla comparsa del banner. In tale contesto, quindi, nel caso in cui l'utente mantenga le impostazioni di default e dunque non acconsenta all'impiego di cookies o altri strumenti di tracciamento, così come nel caso in cui abbia acconsentito solo all'impiego di alcuni cookies o altri strumenti di tracciamento, tale scelta dovrà essere debitamente registrata e la prestazione del consenso non più nuovamente sollecitata se non quando mutino significativamente una o più condizioni del trattamento e quando siano trascorsi almeno 6 mesi dalla precedente presentazione del banner.

Il consenso al momento del primo accesso al sito dovrà comunque essere esclusivamente una manifestazione positiva (cd. opt-in) e non potrà mai riferirsi invece all'espressione di un diniego (cd. opt-out).

L'adeguatezza e la congruità delle caratteristiche del banner (dimensioni, posizionamento, colori, etc.), dovranno essere valutate anche in relazione ai diversi dispositivi di possibile utilizzo da parte dell'Interessato.

A tal fine, è preferibile usare una **grafica** che contrasti con lo sfondo e sia ben leggibile in ogni sua parte, senza differenze estetiche tra le opzioni. In caso di banner strutturati su più livelli, le opzioni di accettazione e quelle di rigetto devono essere presenti entrambe in ogni livello.

L'assenza di un comando di rigetto/rifiuto/diniego/ chiusura è considerata una violazione della normativa sulla privacy.

Qualora l'utente scegliesse di non prestare il proprio consenso al posizionamento dei cookies o all'impiego di altre tecniche di tracciamento, dovrebbe dunque poter limitarsi a chiudere il banner mediante selezione dell'apposito comando usualmente utilizzato a tale scopo, cioè quello contraddistinto da una "**X"** posizionata di regola, e secondo prassi consolidata, in alto a destra e all'interno del banner medesimo, senza essere costretto ad accedere ad altre aree o pagine a ciò appositamente dedicate. Tale comando dovrà avere una evidenza grafica pari a quella degli ulteriori comandi o pulsanti idonei ad esprimere le altre scelte nella disponibilità dell'utente. Le modalità di prosecuzione nella navigazione senza prestare alcun consenso dovranno essere immediate, usabili e accessibili quanto quelle previste per la prestazione del consenso.

Il banner dovrà pertanto contenere, oltre alla X in alto a destra di cui è stata già illustrata la funzione, almeno **le seguenti indicazioni ed opzioni**:

- l'avvertenza che la chiusura del banner mediante selezione dell'apposito comando contraddistinto dalla X posta al suo interno, in alto a destra, comporta il permanere delle impostazioni di default e dunque la continuazione della navigazione in assenza di cookies o altri strumenti di tracciamento diversi da quelli tecnici;
- una informativa minima relativa al fatto che il sito utilizza – se così è ovviamente - cookies o altri strumenti tecnici e/o di profilazione;
- che i cookies o altri strumenti tecnici di profilazione saranno usati esclusivamente previa acquisizione del consenso dell'utente da prestarsi con modalità da indicarsi nella medesima informativa minima che descriva la finalità di trattamento;
- il collegamento ad una informativa estesa posizionata in un secondo livello del banner o in un'apposita pagina del sito, accessibile con un solo click anche tramite un ulteriore link posizionato **nel footer di qualsiasi pagina** del dominio cui l'utente accede;
- un comando attraverso il quale sia possibile esprimere il proprio consenso accettando il posizionamento di tutti i cookies o l'impiego di eventuali altri strumenti di tracciamento;

Le informative per i cookies di profilazioni sono due:

- informativa minima
- informativa estesa

- un comando attraverso il quale sia possibile negare e/o revocare il proprio consenso che abbia la stessa visibilità di quello relativo all'espressione del consenso;
- il link ad una ulteriore area dedicata nella quale sia possibile selezionare, in modo analitico, soltanto le funzionalità, i soggetti cd. terze parti - il cui elenco deve essere tenuto costantemente aggiornato, siano essi raggiungibili tramite specifici link ovvero anche per il tramite del link al sito web di un soggetto intermediario che li rappresenti - ed i cookies, anche eventualmente raggruppati per categorie omogenee, al cui utilizzo l'utente scelga di acconsentire.

Nell'eventualità in cui sia prevista la sola presenza di cookie tecnici o altri strumenti analoghi, di essi potrà essere data informazione nella homepage o nell'informativa generale senza l'esigenza di apporre specifici banner da rimuovere a cura dell'utente.

Il banner non deve essere configurato in modo tale da far apparire l'accettazione del consenso come necessario per continuare nella navigazione sul sito.

Gli utenti dovranno essere posti in condizione di modificare le scelte compiute – sia in termini negativi che in termini positivi e dunque prestando un consenso negato o revocando un consenso prestato – in ogni momento e ciò in maniera semplice, immediata e intuitiva attraverso un'apposita area da rendere accessibile attraverso **un link da posizionarsi nel footer del sito** e che ne renda esplicita la funzionalità attraverso l'indicazione di "*rivedi le tue scelte sui cookies*" o analoga.

Per assicurare che gli utenti non siano influenzati ovvero penalizzati da scelte di design che inducano a preferire una opzione anziché l'altra, si sottolinea inoltre l'esigenza dell'utilizzo di comandi e di caratteri di uguali dimensioni, enfasi e colori, che siano ugualmente facili da visionare e utilizzare.

Resta inteso che i soggetti terzi che forniscono al publisher il servizio di *web measurement*, non dovranno comunque combinare i dati, anche così minimizzati, con altre elaborazioni né trasmetterli a loro volta ad ulteriori terzi, pena l'inaccettabile incremento dei rischi di identificazione dell'utente.

L'informativa generale e quella sui cookies, qualora distinta dalla prima, nonché i comandi per la gestione del consenso, devono essere rapidamente raggiungibili attraverso un link che deve essere visibile da ogni pagina del sito web.

Dei cookies, siano essi strettamente necessari per le finalità di navigazione ovvero funzionali alle ulteriori finalità, deve essere tenuta traccia mediante redazione di una lista costantemente aggiornata in modo da essere tempestivamente fornita all'Autorità di controllo ove richiesta.

****