AZIENDA AUTONOMA DI STATO PER I LAVORI PUBBLICI
Via 28 Luglio, 50 - 47893 BORGO MAGGIORE - REP. SAN MARINO
Tel. 0549 883111 - Fax 0549 883600 - e-mail: segreteria@aaslp.sm
Cod. Op. Econ. SM 02461

Modello organizzativo aziendale

Indice

1. Principi generali

1.1 Oggetto e finalità

1. Il presente documento definisce il Modello organizzativo ed evidenzia le linee-guida e le procedure che l'Azienda Autonoma di Stato per i Lavori Pubblici (di seguito anche brevemente "AASLP") ha adottato al fine di disciplinare i trattamenti di dati personali (ivi compresi quelli particolari) dalla stessa effettuati. I trattamenti di dati personali devono svolgersi nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Ogni trattamento di dati personali effettuato da AASLP deve rispettare le disposizioni contenute nella Legge 21 dicembre 2018 n. 171 (di seguito anche "Legge RSM" o Normativa di riferimento).

3. Il Regolamento Europeo 679/2016 (GDPR) è utilizzato da AASLP esclusivamente come best practices. Infatti, i trattamenti di dati personali effettuati da AASLP non rientrano nell'ambito di applicazione del GDPR (riferimento articolo 3, paragrafo 2).

1.2 Definizioni

1. Ai fini delle disposizioni contenute nella Normativa di riferimento, e tenuto conto dell'organizzazione di AASLP, di seguito sono elencate le principali definizioni:

a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
b) «**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;
c) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
d) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
e) «**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;
f) «**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;

g) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
h) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
i) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
j) "**soggetti autorizzati":** chiunque agisca sotto l'autorità del titolare del trattamento e che abbia accesso a dati personali non può trattare tali dati se non è istruito e autorizzato in tal senso dal titolare del trattamento**;**
k) "interessato": la persona fisica a cui si riferiscono i dati personali;
l) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
m) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
n) **"dati particolari"**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
o) **"dati giudiziari"**: dati personali relativi alle condanne penali e ai reati;
p) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
q) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
r) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
s) "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
t) "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
u) "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

1.3 Principi applicati ai trattamenti

1. AASLP persegue gli obiettivi di sicurezza delle informazioni, dei dati personali, nell'ambito della loro gestione logica, fisica ed organizzativa. Questo comporta l'adozione di un servizio di gestione e protezione dati personali sicuro ed efficiente, che rispetti i principi previsti dalla Normativa di riferimento:

a) "**Responsabilizzazione**" del Titolare del trattamento: garanzia di un'adeguata sicurezza dei dati personali trattati, compresa la protezione, mediante misure tecniche ed organizzative "adeguate" che

siano in grado di mantenere l'integrità, la riservatezza e la disponibilità dei dati; il Titolare del trattamento deve decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative. Ciò presuppone un approccio integrato, che coinvolga tutte le aree dell'organizzazione di AASLP, concreto e risk-based.

b) **Liceità del trattamento**: significa effettuare le operazioni di trattamento dei dati personali nel rispetto di una delle basi giuridiche e di legittimità previste dalla Normativa di riferimento (consenso esplicito, misure precontrattuali, obblighi contrattuali, obblighi legali, compito di interesse pubblico, salvaguardia di interessi vitali, legittimi interessi);
c) **Correttezza del trattamento**: significa adottare forme di lealtà e buona fede in tutte le fasi relative al contesto del trattamento di dati personali, comprese quelle preparatorie e decisori, con particolare attenzione alle modalità per l'interessato di esercitare i propri diritti;
d) **Trasparenza del trattamento**: significa dare tutte le informazioni inerenti ai trattamenti agli interessati in forma concisa, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro;
e) **Limitazione delle finalità di trattamento**: Garanzia rispetto alla gestione e raccolta dei dati per le sole finalità contrattuali, determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Tali garanzie sono applicate e verificate anche a cascata nei confronti degli eventuali fornitori e subfornitori;
f) **Adeguatezza, pertinenza e limitazione** dei dati trattati nel rispetto delle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
g) **Esattezza** dei dati trattati, garantendo in modo tempestivo all'interessato la cancellazione, la rettifica e l'aggiornamento dei dati inesatti;
h) **Limitazione della conservazione** dei dati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("data retention policy");

1.4 Ambito di applicazione

1. Il presente documento si applica a tutta l'organizzazione aziendale, al personale interno, ai dirigenti e le più alte cariche aziendali che devono diffondere la consapevolezza e l'importanza delle tematiche inerenti ai trattamenti di dati personali.

2. Il presente documento è direttamente applicabile a tutti i trattamenti di dati personali effettuati da AASLP, in qualità di Titolare del trattamento/Responsabile del trattamento, nonché a quelli effettuati da soggetti esterni per conto di AASLP.

2. Organizzazione aziendale

2.1 Ruoli privacy

1. La normativa di riferimento definisce alcune figure che ricoprono ruoli e si assumono specifiche responsabilità nell'ambito dei trattamenti di dati personali:

a) Il Titolare del trattamento.
b) Il Responsabile della protezione dei dati personali ("RPD o DPO").
c) I soggetti "autorizzati" del trattamento (autorizzati di primo e secondo livello).
d) I responsabili esterni del trattamento.

2. In aggiunta ai soggetti sopraindicati, pur non essendo previsti espressamente in particolare dalla Legge RSM, è possibile individuare anche:

a) i soggetti autorizzati di "primo livello", ai quali a seconda dell'assetto organizzativo interno, è possibile attribuire specifici compiti e funzioni connessi al trattamento di dati personali.

b) Uno o più amministratori di sistema, ovvero la figura professionale che si occupa della gestione e della manutenzione di un impianto di elaborazione o di sue componenti.

3. Ai fini della struttura organizzativa aziendale, sono da considerare soggetti autorizzati (primo e secondo livello) tutti i dipendenti di AASLP, indipendentemente dal contratto collettivo di appartenenza.

4. L'organizzazione aziendale in termini di risorse umane che svolgono un ruolo attivo nell'ambito del Modello Organizzativo privacy è rappresentata dall'Organigramma privacy aziendale, allegato al presente documento (*Allegato A*).

2.2 Titolare del trattamento

1. Il Titolare del trattamento è l'Azienda Autonoma di Stato per i Lavori Pubblici, nella figura del Presidente del Consiglio di Amministrazione, in qualità di legale rappresentante e in ottemperanza a quanto disposto dalla Delibera del Congresso di Stato n. 5 del 11 marzo 2019.

2. L'ambito di titolarità di trattamento dell'AASLP è circoscritto ai trattamenti in cui vige l'autonomia decisionale nella definizione di finalità e mezzi di trattamento (es: basi giuridiche, soggetti autorizzati, misure e modalità di trattamento).

3. Il Titolare del trattamento con apposito atto giuridico ha delegato al Direttore Generale le seguenti attività:

a) adottare, nelle forme previste dal proprio ordinamento, gli interventi necessari al fine di adeguare l'organizzazione aziendale alle disposizioni della Legge RSM per la protezione dei dati personali;
b) designare i soggetti autorizzati al trattamento dei dati personali;
c) designare i soggetti autorizzati di primo livello a seconda della struttura organizzativa adottata;
d) designare i responsabili esterni del trattamento;
e) designare gli amministratori di sistema;
f) effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il Responsabile della protezione dati designato;

2.3 Responsabile della protezione dei dati personali

1. L'AASLP ha nominato un Responsabile della protezione dei dati personali esterno (di seguito anche "RPD") in ottemperanza a quanto disposto dalla Delibera del Congresso di Stato n. 5 del 11 marzo 2019, domiciliato presso la sede del Titolare e contattabile per ogni questione attinente ai trattamenti di dati personali utilizzando il recapito di posta elettronica indicato nelle informative presenti sul sito istituzionale dell'AASLP.

2. La nomina del RPD è stata comunicata al Garante della protezione dei dati personali. Per lo svolgimento dei propri compiti il RPD è supportato dal personale assegnato in collaborazione dalle diverse strutture (autorizzati di primo livello). I dati di contatto del RPD dell'AASLP sono pubblicati nella sezione internet dedicata alla privacy e nelle rispettive informative.

3. Il RPD svolge i compiti demandategli dalla normativa, nonché quelli indicati nella lettera d'incarico. Il Titolare assicura che il RPD sia coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine il RPD deve disporre tempestivamente di tutte le informazioni pertinenti le decisioni che impattano sul trattamento e sulla protezione dei dati, in modo da poter rendere una consulenza idonea. Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o altro incidente che comporti un rischio per i diritti e le libertà degli Interessati.

4. I documenti e i verbali emessi dal RPD sono conservati da AASLP in apposita repository elettronica il cui accesso è consentito esclusivamente al Direttore Generale e agli autorizzati di primo livello appositamente nominati.

2.4 Autorizzati di primo livello

1. L'Azienda Autonoma di Stato per i Lavori pubblici ha ritenuto opportuno individuare alcuni soggetti cd. autorizzati di primo livello, quali soggetti appositamente designati sulla scorta del proprio assetto organizzativo. L'autorizzato di primo livello coadiuva il Titolare e il Direttore Generale, limitatamente alle sue funzioni, nella definizione delle finalità, delle modalità di trattamento e dei mezzi atti a garantire l'osservanza della normativa sulla protezione dei dati personali. L'autorizzato di primo livello altresì effettua trattamenti di dati personali sulla base di istruzioni scritte del Titolare e del Direttore Generale.

2. Gli Autorizzati di primo livello sono stati individuati nelle seguenti funzioni:

a) Responsabile Unità Operativa (Amministrazione, Acquisti, Personale);
b) Dirigente Settore Edilizia;
c) Dirigente Settore Viabilità e Bonifiche;
d) Dirigente Settore Progettazioni.
e) Dirigente Settori Speciali.

3. L'Autorizzato di primo livello, opportunamente informato dal Direttore Generale:

a) assiste lo stesso Direttore nell'adozione delle procedure in ottemperanza al Modello Organizzativo Privacy, nonché in ogni altra attività o intervento richiesto al fine di adeguare l'organizzazione aziendale alle disposizioni normative in materia di protezione dei dati personali.
b) comunica preventivamente al Titolare del trattamento e al RPD, informando il Direttore Generale, eventuali nuovi trattamenti di dati personali, la cessazione di trattamenti in corso, l'acquisizione di nuove tecnologie che prevedano il trattamento dei dati personali;
c) comunica tempestivamente al RPD, informando il Direttore Generale, eventuali casi di violazione dei diritti della libertà delle persone fisiche;
d) individua i soggetti autorizzati di secondo livello, dando istruzioni specifiche in conformità alle disposizioni di legge.

4. AASLP conserva e aggiorna un elenco dei soggetti autorizzati di primo livello, unitamente ai rispettivi profili di autorizzazione.

2.5 Autorizzati di secondo livello

1. I soggetti autorizzati di primo livello individuano gli autorizzati al trattamento (secondo livello), I soggetti autorizzati di secondo livello sono individuati in tutti i soggetti, diversi da quelli di primo livello, che sono autorizzati a compiere operazioni di trattamento dati su istruzione scritta del Titolare ai sensi dell'art. 30 della Legge RSM. Gli autorizzati di secondo livello al trattamento dei dati all'interno dell'AASLP sono tutti coloro che quotidianamente gestiscono i dati, su supporto sia cartaceo sia informatico (capo sezione, collaboratori tecnici e amministrativi, operatori tecnici e amministrativi, direttori lavori, capisquadra, addetti di segreteria, esperto legale, responsabile sicurezza sul luogo di lavoro interno all'Azienda etc).

2. Gli Autorizzati di secondo livello devono trattare i dati personali, ai quali hanno accesso, attenendosi alle istruzioni del Titolare e del RPD, avendo cura della natura e finalità dei trattamenti svolti, delle tipologie di dati personali oggetto di trattamento e delle misure tecnico organizzative attuate per la corretta protezione dei dati personali.

3. Gli Autorizzati di secondo livello, che di norma sono i soggetti afferenti alla struttura di riferimento di ogni Autorizzato di primo livello, sono adeguatamente formati e ricevono al momento della designazione specifiche istruzioni.

4. Nel dettaglio, gli Autorizzati di secondo livello sono tenuti a:

a) mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante la stessa;
b) non comunicare senza legittima autorizzazione a terzi o comunque diffondere, con o senza l'ausilio di strumenti elettronici, notizie, informazioni o dati appresi, relativi a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di soggetto incaricato/autorizzato e per effetto delle attività svolte;
c) frequentare i corsi d'informazione e formazione in materia di protezione dei dati personali e a sostenere i relativi test conclusivi finalizzati alla verifica dell'apprendimento;
d) segnalare con tempestività al proprio autorizzato di primo livello eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare le procedure di notificazione delle violazioni di dati al Garante Privacy e ai soggetti Interessati.

5. AASLP conserva e aggiorna un elenco dei soggetti autorizzati al trattamento, unitamente ai rispettivi profili di autorizzazione.

2.6 Servizio ICT e Amministratore di Sistema

1. Non essendo presente un apposito servizio ICT all'interno di AASLP, le relative funzioni sono demandate a soggetti esterni, che agiscono in qualità di Responsabili esterni e Amministratori di Sistema.

2. Il ruolo svolto da tali soggetti è di estrema importanza per quanto riguarda l'adozione delle policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario; tali figure svolgono, altresì, un ruolo di supporto al RPD in tema di risorse strumentali e di competenze. La struttura è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto dei principi di accountability, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità alla Normativa di riferimento da parte del RPD.

3. La struttura è tenuta anche a:

a) gestire gli incidenti di sicurezza, assicurando la partecipazione del RPD;
b) individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del RPD;
c) segnalare tempestivamente al RPD le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 34 della Legge RSM.

4. Gli Amministratori di Sistema sono i soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione di dati o di sue componenti, ai sensi del Provvedimento del Garante Privacy del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - doc. web n. 1577499). Tali funzioni devono essere debitamente nominate e periodicamente verificate. L'Amministratore di Sistema ricopre un ruolo delicato: progetta, sviluppa e gestisce l'infrastruttura di rete, i server, i software ed i servizi applicativi di base occupandosi della sicurezza e della protezione dei dati e delle risorse. Di seguito sono prescritti gli adempimenti in ottemperanza al provvedimento indicato sopra:

a) L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
b) la designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
c) gli estremi identificativi delle persone fisiche amministratori di sistema, ivi compresi i nominativi degli amministratori di sistema relativi ai servizi esternalizzati, devono essere riportati, unitamente all'elenco delle funzioni ad essi attribuite, in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
d) L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica, in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.
e) Gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema devono essere idoneamente registrati; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste e devono essere conservate per un periodo non inferiore a sei mesi.

5. AASLP conserva e aggiorna un elenco dei propri Amministratori di sistema, unitamente ai rispettivi profili di autorizzazione.

2.7 Responsabili del trattamento

1. AASLP provvede a designare i Responsabili del trattamento di dati personali, ovvero i soggetti esterni all'organizzazione aziendale che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamento di dati personali per conto del Titolare.

2. Prima di affidare un incarico che prevede un trattamento di dati personali ad un soggetto esterno, AASLP effettua una valutazione in merito all'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del fornitore, affinché lo stesso sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

3. Data la natura contrattuale e negoziale delle attribuzioni del ruolo di responsabile esterno del trattamento, la nomina è effettuata utilizzando apposita modulistica contrattuale, integrata nel Modello Organizzativo privacy adottato dall'AASLP.

4. I Responsabili del trattamento possono nominare dei sub-responsabili, purché autorizzati preventivamente dall'AASLP. In tal caso il Responsabile vincola il sub-responsabile con un contratto (o altro atto giuridico conforme del diritto sammarinese) che contenga gli stessi obblighi previsti nel contratto tra il Responsabile e l'AASLP. Il Responsabile iniziale conserva nei confronti dell'AASLP l'intera responsabilità degli adempimenti degli obblighi del sub-responsabile.

5. AASLP conserva e aggiorna un elenco dei soggetti "Responsabili del trattamento", connesso ai trattamenti affidati a ciascun soggetto.

2.8 Altri ruoli

1. I **membri del Consiglio di Amministrazione**, con esclusione del Presidente, in quanto componenti dell'organo amministrativo aziendale, sono da considerare quali soggetti autorizzati dal Titolare, ai sensi dell'art 30 della Legge RSM. Sono tenuti a rispettare le disposizioni indicate nel precedente capitolo 2.5 e sono nominati a cura del Direttore Generale.

2. I **membri del Collegio Sindacale**, in quanto componenti dell'organo di controllo aziendale, sono da considerare quali Titolari autonomi.

3. Il **Medico del Lavoro** nominato dal Datore di Lavoro in ottemperanza alle disposizioni contenute nella Legge 18 febbraio 1998 n.31, è da considerarsi quale **autonomo titolare del trattamento**. Come si evince dalla nota del Garante italiano del 19 marzo 2019 in risposta ad un quesito posto dalla Società Italiana di Medicina del Lavoro, il Medico del Lavoro tratta i dati personali particolari (dati sullo stato di salute dei dipendenti) per le finalità di cui alla normativa di settore in qualità di Titolare autonomo del trattamento.

3. Politica generale sui trattamenti di dati personali

3.1 Data mapping

1. AASLP effettua rispettivamente i seguenti principali macroprocessi e processi di trattamento dei dati personali:

a) Attività di trattamento svolti dalla Segreteria Generale.
   i. Pubblicazione dei documenti cda e comunicazione dati PA (Amministrazione trasparente)
   ii. Gestione documentale in entrata e uscita
   iii. Gestione dei protocolli documentali.
b) Attività di trattamento in ambito contabile/amministrativo.
   i. Contabilità e bilancio
   ii. Gestione amministrativa e contabile dei dipendenti
   iii. Gestione amministrativa dei documenti del Cda
   iv. Gestione dei sinistri o infortuni dipendenti sul luogo di lavoro.
c) Attività di trattamento in ambito di gestione del personale dipendente.
   i. Gestione del personale stipendiato
   ii. Gestione del personale salariato
d) Accesso ai documenti amministrativi
   i. Gestione dei procedimenti amministrativi
   ii. Gestione delle richieste di accesso ai documenti amministrativi
   iii. Gestione delle richieste di accesso civico
e) Attività di trattamento in ambito di appalti pubblici.
   i. Gestione degli acquisti e appalti di servizi
   ii. Gestione degli incarichi professionali
f) Attività di trattamento in ambito di prestazioni tecnico-operative
   i. Gestione del personale di cantiere (contabilità di cantiere)
   ii. Controllo dei dati relativi all'ubicazione dei mezzi spazza neve
g) Attività di trattamento in merito al sistema informativo aziendale
   i. Gestione dei dati di dominio
   ii. Gestione dei profili di autorizzazione
   iii. Gestione degli strumenti di comunicazione (posta elettronica, tNotice, sito internet)
   iv. Salvataggio e conservazione delle copie delle banche dati aziendali.
   v. Controllo accessi mediante marcatemporale.
   vi. Controllo accessi mediante nuove modalità di timbrature mobile

2. L'attività di mappatura dei trattamenti è stata svolta in una prima fase di adeguamento dell'organizzazione aziendale alle disposizioni normative. Nell'ottica del miglioramento continuo, tale attività è sottoposta a controlli periodici con cadenza semestrale da parte del RPD.

3. L'attività di mappatura dei trattamenti consente dunque anche la puntuale individuazione dei dati personali oggetto di trattamento, essenziale al fine di valutare i rischi in termini di violazione dei dati personali per l'organizzazione aziendale e per gli interessati coinvolti nei trattamenti.

4. La documentazione a supporto dell'attività di mappatura dei processi di trattamento è conservata da AASLP in apposita repository elettronica il cui accesso è consentito esclusivamente al Direttore Generale e ai soggetti autorizzati di primo livello appositamente nominati. La repository elettronica è mantenuta garantendo il rispetto dei parametri di integrità, disponibilità e riservatezza. Le eventuali copie cartacee sono conservate in appositi armadi chiusi a chiave e sono distrutte nel caso in cui non vi sia alcuna utilità o finalità di conservazione in formato cartaceo.

3.2 Registro delle attività di trattamento

1. L'attività di mappatura dei trattamenti e dei dati processati da AASLP è propedeutica alla redazione dei Registri delle attività di trattamento. Il ciclo di vita del dato deve essere individuato per ogni processo di trattamento e rappresenta una delle più efficaci misure organizzative aziendali anche in ottica di individuazione e trattamento dei rischi connessi ai trattamenti.

2. I registri delle attività di trattamento di AASLP contengono le seguenti informazioni inerenti ai processi di trattamento:

a) Identificazione e dati di contatto del Titolare/Responsabile del trattamento.
b) Dati di contatto del RPD.
c) I trattamenti di dati personali (identificabili univocamente da un codice ID).
d) Le finalità e le basi giuridiche di trattamento.
e) Gli interessati coinvolti nei trattamenti.
f) Le tipologie di dati personali oggetto di trattamento.
g) L'eventuale trasferimento dei dati verso un Paese Terzo o un'organizzazione internazionale.
h) I tempi di conservazione dei dati personali.
i) I soggetti interni ed esterni che interagiscono nell'ambito dei trattamenti di dati personali.
j) Gli asset fisici e telematici su cui si fondano i trattamenti.
k) Le misure di sicurezza applicate ai trattamenti al fine di mitigare il verificarsi di rischi di violazione dei dati personali.

3. I registri delle attività di trattamento sono sottoscritti anche digitalmente dal Presidente del Consiglio di Amministrazione in modo da consentire che sia verificabile la data di compilazione, la data di aggiornamento e la data di sottoscrizione degli stessi documenti.

4. La conservazione dei registri delle attività di trattamento nella versione modificabile è effettuata su supporti telematici in apposita repository il cui accesso è consentito esclusivamente al Direttore Generale e agli autorizzati di primo livello appositamente nominati.

5. La conservazione dei registri delle attività di trattamenti sottoscritti dal Presidente del Consiglio di Amministrazione è effettuata:

a) su supporti telematici, protetti da profili di autorizzazione, in modo da garantire l'accesso esclusivo al Direttore Generale e ai soggetti autorizzati di primo livello.
b) Su supporti cartacei, in appositi armadi chiusi a chiave.

6. I Registri delle attività di trattamento sono messi a disposizione dell'Autorità Garante per la protezione dei dati personali, su richiesta o in ossequio a ispezione e controlli.

7. I Registri delle attività di trattamento sono sottoposti a controlli e verifiche periodiche con cadenza trimestrale da parte del RPD.

3.3 Analisi dei rischi

1. Il trattamento di dati personali rappresenta un'attività pericolosa, in quanto in grado di generare delle conseguenze dannose sia nei confronti di AASLP che degli interessati coinvolti nei trattamenti. Per tale ragione AASLP prima di effettuare dei trattamenti di dati personali, procede ad analizzarne i rischi inerenti (cd. Risk based approach).

2. Integrato al sistema di analisi e trattamento dei rischi, nonché al Modello organizzativo privacy, AASLP prevede l'adozione di una procedura che definisca quando e in che modo un nuovo trattamento di dati personali debba essere intrapreso.

3. L'attività di analisi e trattamento dei rischi è effettuata sulla base delle informazioni presenti negli stati di fatto IT, archivistici e logistici di AASLP, nei quali sono indicate le misure di sicurezza già implementate dall'organizzazione aziendale. Tali documenti sono oggetto di aggiornamenti costanti, in funzione delle variazioni interne ed esterne apportate da AASLP.

4. Il Sistema di gestione dei rischi connessi alle operazioni di trattamento deve essere documentato e aggiornato costantemente, ogniqualvolta intervengano delle modifiche sui processi di trattamento (finalità, basi giuridiche, mezzi di trattamento, interessati e dati personali), nonché delle variazioni nelle minacce.

3.4 Valutazione d'impatto

1. La valutazione d'impatto ai sensi dell'articolo 36 della Legge RSM è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche, valutando detti rischi e determinandone le misure per affrontarli.

2. AASLP unitamente al sistema di gestione dei rischi connessi ai trattamenti, effettua una valutazione d'impatto ogniqualvolta dall'analisi dei rischi privacy derivano dei rischi elevati per i diritti e le libertà degli interessati coinvolti, tenendo conto in particolare dei trattamenti effettuati in modalità telematica.

3. AASLP interviene con una valutazione d'impatto in tutti i casi elencati nell'Allegato 1 al provvedimento dell'Autorità Garante italiana n.467 del 11/10/2018, nonché nelle fattispecie di trattamento che saranno pubblicate dall'Autorità di controllo della Repubblica di San Marino. In particolare, tenuto conto delle attività caratteristiche svolte da AASLP, si segnalano le seguenti operazioni di trattamento tra quelle sottoposte o da sottoporre a valutazione d'impatto:

a) Trattamenti in ambito lavorativo relative alle timbrature mobile mediante l'utilizzo di nuovi strumenti tecnologici.
b) Scambio su larga scala di dati tra più titolari con modalità telematiche (in particolare per le comunicazioni tra pubbliche amministrazioni)
c) Trattamenti di dati personali effettuati su larga scala.
d) Trattamenti di dati personali particolari e giudiziari.

4. AASLP prima di procedere ad una valutazione d'impatto consulta il Responsabile della Protezione dei dati personali nominato in merito ad un'analisi sulla obbligatorietà o meno di procedervi, sulle modalità con cui effettuarla e su ogni aspetto inerente ai rischi connessi ai diritti e le libertà dell'interessato. Il Responsabile della protezione dei dati personali nominato è tenuto ad emettere un parere in merito agli esiti della valutazione d'impatto condotta dall'AASLP, parere che può essere reso pubblico dalla stessa AASLP a garanzia di trasparenza e correttezza di interessati e stakeholders.

5. AASLP procede ad una revisione e un aggiornamento delle valutazioni d'impatto con cadenza almeno annuale ed ogniqualvolta vi siano cambiamenti nel processo di trattamento censito e in termini di rischi con impatto sui diritti e le libertà degli interessati coinvolti.

3.5 Formazione e istruzione

1. Chiunque agisca sotto l'autorità di AASLP e che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento. AASLP implementa in modo continuativo la formazione del proprio personale dipendente in merito agli adempimenti richiesti dalla normativa di riferimento e ai rischi connessi ai trattamenti di dati.

2. I soggetti autorizzati al trattamento e chiunque agisce sotto l'autorità di AASLP deve ricevere adeguate istruzioni e direttive inerenti alle modalità corrette di trattamento del dato. Tali istruzioni di trattamento devono essere recepite e sottoscritte in modo formale dai soggetti indicati sopra attraverso degli ordini di servizio.

3. I programmi di formazione sviluppati da AASLP sono divisi in due categorie di soggetti:

a) Decisori, ovvero le figure che all'interno dell'organizzazione aziendale assumono decisioni e maggiori responsabilità, quali il Direttore Generale, i Dirigenti, i Responsabili di Unità Operativa e alcuni Capo Sezione.
b) Operativi, ovvero le figure che eseguono le proprie mansioni lavorative su indicazione e istruzione dei decisori, quali i collaboratori di sezione e gli operatori di sezione.

4. Ogni nuova risorsa umana deve essere sottoposta ad un primo ciclo di formazione a seconda del ruolo e delle mansioni svolte. Al termine della formazione, alla risorsa è fornita l'ordine di servizio contenente le corrette istruzioni di trattamento.

5. La formazione del personale dipendente deve presentare le seguenti caratteristiche:

a) Pianificata e programmata.
b) Differenziata per area (decisori e operativi).
c) Granulare (effettuata in più fasi ed in modo costante).
d) Testata e verificata (test di apprendimento).

3.6 Sicurezza dei trattamenti

1. AASLP si impegna a garantire che i trattamenti di dati personali siano effettuati nel rispetto delle disposizioni contenute nella Normativa di riferimento, garantendo la qualità, l'integrità, la riservatezza e la disponibilità del dato.

2. Al fine di garantire il rispetto dei parametri di sicurezza sopraindicati, AASLP adotta o intende implementare le seguenti misure di sicurezza:

a) Procedura di controllo dell'esattezza del dato sulla base di periodici campionamenti.
b) Politica di Autenticazione che prevede l'assegnazione di parole chiave robuste a ciascun utente, una frequenza di cambiamento di 90 giorni, istruzioni sulla conservazione delle copie delle parole chiave, assegnazione del ruolo di custode delle copie delle credenziali in busta chiusa, parole chiavi non riassegnabili, disattivazione delle credenziali di accesso per disuso o perdita della qualità.
c) Politica di autorizzazione degli accessi e di utilizzo dei dati, che prevede l'assegnazione di profili di accesso e utilizzo delle banche dati e dei documenti aziendali a seconda delle mansioni e

responsabilità di ciascun utente, nonché una verifica e aggiornamento annuale del sistema di autorizzazione implementato.

d) Aggiornamento periodico della lista dei soggetti autorizzati.
e) Censimento e aggiornamento periodico di tutti i sistemi hardware e software utilizzati in ambito aziendale o ad uso promiscuo, compresi i supporti removibili.
f) Installazione e aggiornamento periodico dei sistemi operativi presenti su ogni PC in uso e collegato alla rete aziendale.
g) Installazione e aggiornamento automatico e quotidiano di applicativi antivirali su ogni PC in uso e collegato alla rete aziendale.
h) Installazione e aggiornamento periodico di Firewall con funzioni di IPS/IDS.
i) Custodia in luoghi ad accesso controllato dei dispositivi removibili utilizzati nell'ambito delle attività aziendali, o cifratura degli stessi.
j) Protezione fisica dei dati su supporti cartacei (adozione di armadiature chiusi a chiave e gestione sistematica delle copie)
k) Politica di salvataggio dei dati quotidiana e automatizzata, che preveda copie ridondanti di tutti i dati oggetto di trattamento su tre livelli di supporti, e conservazione dei supporti di salvataggio in luoghi diversi tali da garantire un adeguato grado di disponibilità del dato.
l) Installazione di un software di logging per la conservazione e il monitoraggio degli accessi alla rete aziendale ed in particolare per il monitoraggio degli Amministratori di sistema.
m) Politica di scambio di comunicazione elettroniche che si basi sulla cifratura delle comunicazioni (Protocollo SSL) e sulla cifratura dei dati o dei documenti che contengono ogniqualvolta si comunichino dati particolari e giudiziari.
n) Politica di ripristino del dato che sia in grado di garantire la disponibilità dei dati in tempistiche sostenibili.
o) Nomina degli Amministratori di Sistema, così come definiti dal provvedimento del Garante della protezione dei dati italiano del 27 novembre 2008, nonché conservazione e aggiornamento degli estremi identificativi.
p) Software di cancellazione sicura e definitiva del dato, decorso i termini di conservazione.
q) Politica di disaster recovery che riguardi tutti i dati personali trattati (es: Sistemi Cloud con adeguate misure di sicurezza, certificati ISO 27001)
r) Pseudonimizzazione dei dati personali oggetto di trattamenti che presentano rischiosità maggiori, nonché conservazione sicura e distinta degli elementi identificativi dell'interessato.

3. Le misure di sicurezza adottate da AASLP sono oggetto di modifiche e implementazione in ossequio all'evoluzione dello stato dell'arte della tecnologia, nonché in virtù di modifiche nel contesto interno o esterno all'organizzazione.

3.7 Manuale privacy

1. In ottemperanza alle disposizioni contenute nello schema di certificazione per la valutazione della conformità al GDPR ISDP©10003:2020, AASLP adotta un Manuale privacy, il quale rappresenta un documento sinottico in cui sono illustrate, pianificate e monitorare tutte le procedure e politiche aziendali in materia di trattamento e protezione dei dati personali.

2. Il Manuale privacy adottato da AASLP è integrato dal presente documento e dalle seguenti politiche e procedure aziendali:

a) Procedura per iniziare un nuovo trattamento
b) Istruzioni e Linee guida per la redazione dell'analisi e del trattamento del rischio
c) Istruzioni e Linee guida per la redazione di una valutazione d'impatto.
d) Istruzioni e Linee guida sul trattamento dei dati personali.

e) Politica generale sulla sicurezza del trattamento (misure espresse nel precedente capitolo 3.6)
f) Politica di gestione di una violazione di dati personali
g) Politica di gestione di una richiesta di esercizio dei diritti da parte degli interessati.
h) Procedura di selezione di un responsabile esterno del trattamento.
i) Procedura per la gestione di una richiesta di diritto di accesso amministrativo o civico.
j) Procedura per la pubblicazione di dati (Amministrazione trasparente)
k) Procedura per il controllo dell'esattezza, dell'aggiornamento e completezza dei dati personali trattati (Qualità)
l) Politica sulla conservazione dei dati personali.
m) Procedura per la gestione di un'ispezione da parte dell'Autorità di controllo
n) Procedura per la gestione dei trattamenti di dati personali effettuati aventi maggiori rischiosità.

Le presenti politiche e procedure aziendali potranno essere emesse ed implementate in parte anche successivamente alla validazione del Manuale privacy.

3. Il Manuale privacy adottato da AASLP evidenzia ed è integrato, inoltre, dalla seguente documentazione:

a) Informative sul trattamento dei dati personali specifiche per ogni fattispecie di trattamento
b) Lettere d'incarico dei soggetti autorizzati al trattamento
c) Atti di nomina dei responsabili esterni e degli Amministratori di Sistema.
d) Registri delle attività di trattamento.
e) Risultanze delle analisi dei rischi e Registro rischi e DPIA.
f) Report delle valutazioni d'impatto condotte.
g) Registro delle violazioni di dati personali
h) Registro delle richieste di esercizio dei diritti dell'interessato.
i) Report di analisi dei processi aziendali e dei flussi di dati personali.
j) Organigramma privacy e Organigramma aziendale.
k) Verbali emessi dal RDP.

4. Il Manuele privacy corredato dalla relativa documentazione è conservato da AASLP in apposita repository elettronica il cui accesso è consentito esclusivamente al Direttore Generale e agli autorizzati di primo livello appositamente nominati. La repository elettronica è mantenuta garantendo il rispetto dei parametri di integrità, disponibilità e riservatezza. Le eventuali copie cartacee sono conservate in appositi armadi chiusi a chiave e sono distrutte nel caso in cui non vi sia alcuna utilità o finalità di conservazione in formato cartaceo.

5. La singola documentazione può essere comunicata ai soggetti interessati secondo le modalità stabilite dal Direttore Generale al fine di implementare i processi di trattamento.

6. Il Manuale Privacy adottato da AASLP è sottoscritto dal Presidente del Consiglio di Amministrazione ed è sottoposto ad aggiornamenti periodici con cadenza almeno annuale in un'ottica di miglioramento continuo dei processi di adeguamento, al fine di verificarne l'efficacia, l'adeguatezza e la corretta applicazione e comprensione.

3.8 Audit e controlli

1. Il Modello organizzativo privacy adottato da AASLP è sottoposto ad audit e verifiche di conformità sostanziale e documentale da parte del RPD, il quale agisce in qualità di controllore sull'osservanza delle disposizioni di legge previste dalla Normativa di riferimento.

2. Le verifiche del RPD avvengono senza recare un danno all'esecuzione dell'attività aziendale e possono essere effettuate anche senza termini di preavviso.

3. Gli esiti delle verifiche effettuate dal RPD sono documentati in un report che evidenzia i rilievi e le rispettive azioni correttive che AASLP deve adottare, nonché le scadenze temporali di adozione delle stesse al fine di eliminare le cause di non conformità rilevate.

4. Disposizioni finali

4.1 Sanzioni

1. Le violazioni delle disposizioni di cui al presente documento, del Modello Organizzativo privacy, nonché della normativa di riferimento in materia di trattamento dei dati personali sono prese in carico dal Direttore Generale.

2. Per le violazioni compiute dai soggetti autorizzati, i procedimenti disciplinari saranno promossi ai sensi della Legge 31 luglio 2009 n. 106 "Norme di disciplina per i pubblici dipendenti" e dai vigenti contratti di lavoro collettivi, fatte salve le azioni di natura civile e penale."

4.2 Entrata in vigore

1. Il presente Regolamento entra in vigore dalla data di emanazione e sottoscrizione da parte del Presidente del Consiglio di Amministrazione di AASLP del Manuale privacy indicato nel capitolo 3.7, previa delibera favorevole del Consiglio di Amministrazione.

2. Ogni altro documento emesso da AASLP in difformità a quanto indicato nella presente politica è abrogato.

4.3 Disposizioni integrative

1. Per quanto non espressamente previsto dal presente documento, si rinvia alla normativa generale vigente, con particolare riferimento alla Legge 21 dicembre 2018 n.171 e al Regolamento UE 2016/679, e successive modificazioni.

2. Le determinazioni delle Autorità di controllo sammarinese e italiana, anche successive all'entrata in vigore del presente documento, si ritengono automaticamente recepite ed efficaci, se d'impatto per AASLP.

4.4 Monitoraggio e riesame

1. Il presente documento viene adottato nelle more di completamento del quadro normativo in materia di protezione dati personali e potrà essere soggetto a adeguamenti conseguenti ai seguenti fattori:

a) Evoluzioni significative del business;
b) Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
c) Significativi incidenti di sicurezza;
d) Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni

2. Anche a regime, il Modello organizzativo privacy dovrà essere sottoposto a costante monitoraggio, allo scopo di intervenire tempestivamente, anche su proposta del RPD, sull'assetto organizzativo in caso di modifiche normative o a seguito dell'evoluzione tecnologica o della necessità di introdurre nuove e più efficaci politiche di gestione dei dati personali.

Repubblica di San Marino, 12 aprile 2021

Fto. Presidente del Consiglio di Amministrazione

Azienda Autonoma di Stato per i lavori pubblici

Allegato A: Organigramma privacy