REGOLAMENTO INTERNO SUL TRATTAMENTO DEI DATI PERSONALI

Approvato da RPD

PREAMBOLO

1. ASSA S.P.A. adotta il seguente regolamento di condotta al quale tutto il personale si deve attenersi per rispettare le norme e i principi per il corretto trattamento dei dati personali. Il Regolamento (UE) 2016/679 adotta una nuova disciplina sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e abroga la direttiva 95 /46/CE.
2. Il Regolamento europeo (GDPR) obbliga ad adeguarsi alle nuove regole in maniera tale da assicurare un livello elevato di protezione dei dati che riguardano le persone fisiche, equivalente in tutti gli Stati membri, così da rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione.
3. Il regolamento europeo richiama l'articolo 8, paragrafo 1 della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1 del Trattato sul funzionamento dell'Unione europea, nei quali è stabilito che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
4. Per l'attuazione del regolamento U.E. è necessario il diretto coinvolgimento dell' Azienda poiché la normativa europea determina, *in primis* un cambiamento culturale, ponendo al centro del sistema i cittadini ai quali viene riconosciuto un livello elevato e uniforme di tutela dei propri dati personali, oltreché un maggior controllo sull'utilizzo degli stessi, con il riconoscimento di nuovi e più incisivi diritti a favore di ciascun interessato quali il diritto all'oblio, il diritto alla portabilità dei dati, il diritto ad essere informato in modo trasparente, leale e dinamico sui trattamenti effettuati, il diritto ad essere informato sulle violazioni dei propri dati personali, il diritto di essere avvertiti in caso di violazioni dei dati personali entro 72 ore, il diritto a dare mandato ad un organismo apposito per proporre reclamo in caso di violazione dei dati delle disposizioni di regolamento, nonché il diritto ad ottenere tutela risarcitoria in caso di violazione del regolamento.
5. il Regolamento, impone una forte responsabilizzazione poiché la protezione dei dati personali diventa un "asset strategico" ed in quanto tale deve essere valutato prima, già nel momento di progettazione di nuove procedure, prodotti o servizi, (principi "privacy by design" e "privacy by default") e non più un mero adempimento formale.
6. Il regolamento con il principio di "responsabilizzazione" (cosiddetta "accountability"), attribuisce ai titolari del trattamento che determina le finalità e i mezzi del trattamento dei dati personali, il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (articolo 5 del regolamento UE).

7. L'applicazione del principio di responsabilizzazione si lega inscindibilmente al concetto di Privacy by design, ovvero l'individuazione delle concrete misure a tutela dei dati personali a cui si è tenuti a porre in essere oltre alle misure minime e di carattere generale riconducibili al concetto di "privacy by default".
8. Il concetto di "accountability" esprime anche l'obbligo di rendicontazione gravante sull'Azienda, la quale è tenuta a dimostrare di avere adottato le misure di sicurezza adeguate ed efficaci a protezione dei dati degli interessati, nonché che tali misure sono costantemente riviste ed aggiornate e che le attività proprie, in particolare i trattamenti svolti sono conformi con i principi e le disposizioni del Regolamento europeo, in particolare che le misure adottate a fronte dei rischi che corrono i dati forniti dagli interessati sono efficaci ed adeguate, ciò premesso, rilevato che:
le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti e che deve essere effettuata la valutazione d'impatto dal titolare con l'assistenza del RPD, che è essenziale sia per la revisione dei processi gestionali interni all'Ente, finalizzata a raggiungere i più adeguati livelli di sicurezza nel trattamento dei dati personali prescritti dalla normativa europea e rispondenti alle effettive esigenze, nonché alla struttura organizzativa e gestionale del titolare del trattamento che in occasione dell'adozione di nuove misure tecnologiche e di gestione dei dati, come nel caso di specie, tutto ciò premesso si adotta il qui di seguito il presente

REGOLAMENTO

ART. 1 SCOPO E FINALITÀ

1.Il presente regolamento attua in ASSA S.P.A. i principi contenuti nel Regolamento UE 2016/679 in conformità alle norme del D. Lgs.196/2003, come modificato dal D. Lgs. del 10 agosto 2018 n.101 (Codice Privacy), riordina la struttura organizzativa, le responsabilità, le misure tecniche, la comunicazione e la gestione delle diverse tipologie di dati personali, "particolari" e i trattamenti eseguiti da ASSA S.P.A..

2.Il trattamento dei dati in ASSA S.P.A. ha base giuridica nel contratto e nell'esercizio del potere attribuito e per tali attività che ASSA S.P.A. tratta prevalentemente dati personali comuni.

3.I dati personali in ASSA S.P.A. sono trattati in modo lecito, corretto e trasparente e sono raccolti per le finalità determinate dal contratto e dalla legge e dai regolamenti che sono esplicite e legittime, e i trattamenti avvengono in modo non incompatibile con le finalità attribuite.

4.I dati sono trattati da ASSA S.P.A. in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono trattati e di norma secondo il criterio di «minimizzazione dei dati». Dei dati è costantemente verificata l'esattezza e, quando è necessario l'aggiornamento. Nel trattamento ASSA S.P.A. adotta tutte le misure tecniche adeguate e ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

5. La limitazione della conservazione dei dati in ASSA S.P.A. è volta a consentire l'identificazione degli interessati solo per l'arco di tempo necessario nel quale è in atto il trattamento che, di norma, non può essere mai superiore alle finalità per le quali i dati stessi sono trattati.

6. Nel rispetto delle singole leggi di settore che prevedono la conservazione per periodi diversi per quelli stabiliti è possibile la conservazione dei dati per periodi più lunghi in relazione alla tipicità dei singoli procedimenti di legittimo interesse di ASSA S.P.A.

Art. 2 Disposizioni generali

1. ASSA S.P.A. nel trattare i dati osserva la vigente normativa Europea e Nazionale, i pareri del Garante nazionale, le decisone della Commissione Europea e del GEPD. Il trattamento dei dati in ASSA S.P.A. è sempre improntato al rispetto dei diritti e delle libertà fondamentali dell'interessato è per le finalità di interesse pubblico perseguito dall'Ente.

2. ASSA S.P.A. adegua la propria organizzazione interna alla normativa sulla protezione dei dati, in senso verticale con a capo il Direttore Generale.

Art. 3 Definizione di dati personali e dati particolari

1. Ai fini dell'applicazione della normative europea e nazionale a tutela delle persone fisiche e per le legittime attività di trattamento per dato personale si intende 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.
2. Trattamento è qualsiasi singola operazione, svolta dal personale dipendente di ASSA S.P.A., ovvero l'insieme delle operazioni, compiute sia attraverso la forma analogica che digitale e quindi con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come e che consistono nella 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 di dati personali trattati in ASSA S.P.A..
3. IASSA S.P.A. si conforma al divieto del trattamento dei dati "particolari" di cui all'art. 9 del GDPR e, in assenza di previsione derogatoria ovvero dell'espresso consenso dell'interessato, il personale di ASSA S.P.A. si astiene dal trattare dati "particolari" che direttamente o indirettamente siano idonei a far rilevare:

- l'origine razziale o etnica dei soggetti i cui dati vengono trattati;
- le loro opinioni politiche;
- le loro convinzioni religiose o filosofiche;
- l'appartenenza sindacale anche per i dipendenti interni;
- i loro dati genetici;
- i loro dati biometrici che identificano la persona fisica,
- dati relativi alla salute;
- alla vita sessuale o all'orientamento sessuale.

4. ASSA S.P.A. è legittimata a trattare i dati "particolari", di cui al precedente comma 3, quando ricorre una delle seguenti condizioni:
a) l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali per una o più finalità specifiche in relazione ai compiti attribuiti ad ASSA S.P.A.;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici attribuiti all'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, sulla base del diritto dell'Unione o Nazionale, fatte salve le garanzie per i diritti fondamentali e gli interessi dell'interessato;

c)il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato quando questi sono reperibili sul web tramite i motori di ricerca o trasmessi ad ASSA S.P.A. con il Curriculum per la partecipazione a selezioni pubbliche;
e) il trattamento è necessario per ASSA, gli interessati o terzi controinteressati per fare accertare, esercitare o difendere un diritto in sede giudiziaria;
f) il trattamento è necessario per motivi di interesse pubblico rilevante in relazione alle attribuzioni ad ASSA S.P.A.;
g) il trattamento è necessario in quanto è relativo alla raccolta, esame e trasmissione di dati raccolti per le finalità nell'ambito dei compiti attribuiti ad ASSA S.P.A. della capacità lavorativa del dipendente, diagnosi, assistenza;
j) il trattamento è necessario a fini di archiviazione a fini statistici.

Art. 4 Titolare del trattamento

1. Per i trattamenti di legge e la tutela delle persone fisiche per le finalità istituzionali il Direttore Generale è il titolare dei dati personali contenuti nelle banche dati automatizzate o cartacee.
2. Il Direttore Generale determina le finalità e i mezzi del trattamento, predispone le line di Policy Privacy di ASSA S.P.A., adotta il regolamento interno.
3. Il Direttore Generale spetta inoltre il compito di adottare, sentito il DPO, le misure tecniche ed organizzative adeguate volte a garantire un livello di sicurezza al rischio del trattamento dei dati in ASSA S.P.A.
b. Tenere e implementare, anche per mezzo di uno o più dipendenti interni il registro dei trattamenti.
c. Vigilare sul registro delle attività di trattamento in capo ad ogni struttura.
d. Attestare, se richiesto dal Garante o dall'A.G., che i trattamenti sono conformi ai principi e alle disposizioni di legge del Regolamento UE.
e. Monitorare periodicamente, mediante gli amministratori di Sistema, l'efficacia delle misure di sicurezza tecniche e fisiche adottate in ASSA S.P.A. sentito il parere del DPO.
f. Mettere il registro dei trattamenti a disposizione dell'autorità Garante.
g. Nominare i responsabili del trattamento.
h. Stipulare contratti di nomina.
i. Sottoscrive i contratti di contitolarità.
j. Stipula protocolli d'intesa.
k. Organizzare ogni altra attività e attribuire compiti e funzioni.

l. Nomina, ai sensi dell'art. 7, comma 6, D.lgs. 165/2001, nel rispetto delle previsioni del GDPR e tenuto conto delle specifiche competenze e della pregressa esperienza, il Responsabile della protezione dati individua le risorse umane e finanziarie necessarie nonché la struttura per le attività del RPD.
m. Adotta il Piano della sicurezza del patrimonio informativo, le politiche di sicurezza, le metodologie di analisi del rischio privacy e di valutazione di impatto, le linee guida per l'utilizzo dei dispositivi fissi e mobili.
n. Presiede il Gruppo di lavoro per la gestione delle violazioni di dati personali (Data Breach) composto dai responsabili incaricati, l'Amministratore di Sistema, il RPD.
o. Ogni altra questione ad esso demandata in materia di protezione dei dati personali.
p. predispone sentito il RPD i modelli facsimile di lettera di autorizzazione al trattamento dei dati personali e di affidamento della custodia di particolari archivi, chiavi o credenziali di autenticazione e impartisce le relative istruzioni ai soggetti autorizzati al trattamento di dati personali.
q. Autorizzare le strutture ai trattamenti di dati personali nell'ambito delle funzioni attribuire.

Art. 5. I<u>nformativa e consenso</u>

1 Tutti gli uffici devono avere disponibile l'informativa per clienti/fornitori.
2 Gli uffici a contatto con il pubblico devono stampare una informativa e renderla disponibile per la consultazione che deve essere aggiornata al regolamento europeo UE 2016/679.
3. Quando determinati servizi possono essere resi solo sulla base del preventivo consenso dell'interessato, spetta ad dipendente che per primo è tenuto a raccogliere i dati dell'interessato, munirsi di informativa chiara e semplice in calce alla quale deve essere acquisito il consenso mediante sottoscrizione – o altro mezzo equivalente - e previa identificazione dell'interessato.

<u>Art. 6 Liceità del trattamento e riservatezza</u>

1 Il trattamento dei dati deve essere effettuato in modo lecito e corretto in modo pertinente e non eccedente.
2. I dati personali devono essere raccolti e registrati unicamente per finalità inerenti all'attività svolta e devono essere aggiornati e agli stessi devono essere applicate le misure di sicurezza predisposte dal Titolare.
3. Ogni trattamento deve essere garantita la massima riservatezza ed in particolare è fatto divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Titolare, l'accesso è limitato solo per l'espletamento delle mansioni attribuiti durante la prestazione dio lavoro.

Art. 7 Misure di sicurezza

1. Tutti i dispositivi (PC, Smartphone, I.O.T, memorie USB) in dotazione Aziendale ai dipendenti, devono essere dotati di sistemi di protezione, periodicamente scansionati con software o procedure che possano garantire un adeguato livello di sicurezza.
2. E' fatto divieto di utilizzare dispositivi personali se non espressamente autorizzati. E' altresì fatto divieto di lasciare l'ufficio anche per breve periodo senza chiudere le porte a chiave, oppure lasciare documenti non custoditi in armadi o cassetti assicurati con chiusura a chiave.
3. Gli uffici che sono a contatto con il pubblico dovrebbero mantenere tutti i documenti lontani dalla portata degli stessi alle spalle dell'operatore.
4. A fine lavoro è opportuno lasciare le scrivanie vuote e riporre i documenti il luogo sicuro, preferibilmente in armadi o cassettiere.
5. A fine erogazione di un servizio, se la documentazione cartacea non è più necessaria, provvedere alla distruzione dei documenti, utilizzando appositi "distruggi documenti" oppure strappandoli in piccoli pezzi prima di buttarli nel cestino.
6. E' vietato collegare smartphone, tablet e in generale dispositivi dotati di microprocessore alle porte USB dei computers.
7. E' vietato installare software senza autorizzazione da pare dell'amministratore di sistema.
8. E' vietato inoltrare la corrispondenza elettronica in copia (CC) ad indirizzi email che non fanno parte dei domini di posta elettronica utilizzati dall'Azienda, mentre per la comunicazione a più soggetti occorre utilizzare la funzione (CCN) intestando il primo destinatario all'ufficio stesso che spedisce.
9. I monitor degli operatori devono essere posizionati in modo da impedire la lettura da parte del pubblico;
10. Le password non devono mai essere posizionate sui monitor o sui computers;
11. Gli autorizzati al trattamento di particolari categorie di dati personali, devono impostare uno screen saver con password che intervenga al più tardi dopo 2 minuti di inattività;
12. Al verificarsi di comportamenti anomali dei sistemi informativi in dotazione, o commessi errori involontari che possano compromettere la sicurezza della rete informatica, devono essere tempestivamente comunicati al Responsabile della protezione dati e all'amministratore di sistema e al titolare.
13. Prima di lasciare la postazione di lavoro con assenza superiore ai 15 minuti, è necessario chiudere la sessione di lavoro e spegnere il PC.
14. Periodicamente effettuare una scansione manuale con antivirus a fine giornata nei giorni e su istruzione dell'amministratore di sistema.

Art. 8 Pubblicazione online

1. I soggetti pubblici possono diffondere dati personali solo se ciò è ammesso da una specifica disposizione di legge o di regolamento.

2. Dopo aver verificato la sussistenza dell'obbligo di pubblicazione dell'atto o del documento nel proprio sito web istituzionale, il soggetto pubblico deve limitarsi a includere negli atti da pubblicare solo quei dati personali realmente necessari e proporzionati alla finalità di trasparenza perseguita nel caso concreto. Se sono particolari (ossia idonei a rivelare ad esempio l'origine razziale ed etnica, le convinzioni religiose, le opinioni politiche, l'adesione a partiti o sindacati, lo stato di salute e la vita sessuale) o relativi a procedimenti giudiziari, i dati possono essere trattati solo se indispensabili, ossia se la finalità di trasparenza non può essere conseguita con dati anonimi o dati personali di natura diversa e comunque nel rispetto dell'art. 9 del GDPR 2016/679 dell'art. 2-sexies del D.Lgs. 196/2003 e delle linee guida del garante privacy del 2014.
3. Prima di procedere alla pubblicazione sul proprio sito web si deve:
- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;
- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;
- sottrarre all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) i dati sensibili e giudiziari, come ricordati al punto precedente.
4. È vietato diffondere dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici. Il Garante ha più volte ribadito la necessità di garantire il rispetto della dignità delle persone, facendo oscurare, ad esempio, dai siti web di diversi Comuni italiani i dati personali contenuti nelle ordinanze con le quali i sindaci disponevano il trattamento sanitario obbligatorio per determinati cittadini.
5. Quando è possibile, preferire l'anonimizzazione dei dati dell'interessato. Per anonimizzare un documento non basta sostituire il nome e cognome con le iniziali dell'interessato ma occorre oscurare del tutto il nominativo e le altre informazioni riferite all'interessato che ne possono con-sentire l'identificazione anche a posteriori (es. numero protocollo ecc.).

Art. 9 Registro delle attività di trattamento

1. Il Direttore Generale tiene, sotto la propria responsabilità, il Registro delle attività di Trattamento la cui compilazione e implementazione può assegnare a un interno.
2. Il Registro del titolare, è redatto in forma scritta, anche in formato elettronico, ed è messo a disposizione, a richiesta, dell'Autorità Garante per la Privacy, per ispezioni e controlli ai fini della correttezza nella gestione e trattamento dei dati personali

Art. 10 Responsabile (designato) al trattamento

1. I Responsabili (designato) al trattamento sono individuati dal D.G. La mancata accettazione della nomina costituisce illecito contrattuale.
2. Il responsabile(designato) adempie agli obblighi di trasparenza e vigilanza, prescritti dal titolare nell'atto giuridico di nomina mettendo a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi imposti.
3. Il responsabile del trattamento (designato) coadiuva il titolare nell'adozione delle misure tecniche e organizzative imposte dai processi di innovazione tecnologica.
4.Indica al titolare, sentito il RPD, alcune misure di sicurezza utili per ridurre i rischi del trattamento, quali la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali.
5. Il responsabile ha l'obbligo, d'intesa con il RPD, di avvisare, assistere e consigliare il titolare ed è tenuto a consentire e contribuire alle attività di revisione, comprese le ispezioni e *audit,* realizzate dal titolare del trattamento.

Art. 11 Incaricati del trattamento

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

Art. 12 Responsabile del trattamento dati informatici e telematici (D.I.T.)

1. La responsabilità del trattamento dei dati informatici e telematici è attribuita al Responsabile dei Sistemi Informativi e Servizi Informatici. Le competenze del Responsabile riguardano l'attività di controllo e gestione degli impianti di elaborazione o di sue componenti, di basi di dati, di reti, di apparati di sicurezza e di sistemi di software complessi (nella misura in cui consentono di intervenire su dati), l'individuazione e attuazione di tutte le procedure fisiche, logiche e organizzative per tutelare la sicurezza e la riservatezza nel trattamento dei dati informatici.

2. Il Responsabile del trattamento dati informatici e telematici designa per iscritto con provvedimento motivato, un numero limitato, di amministratori di sistema e di amministratori di macchina, previa individuazione delle caratteristiche di esperienza, capacità e 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.
3.Il Responsabile del trattamento dati informatici e telematici predispone - per le parti relative alla sicurezza informatica, ai trattamenti di dati personali con mezzi elettronici e digitali e allo sviluppo delle applicazioni informatiche - proposte per il:
a. Piano della sicurezza del patrimonio informativo e della protezione dei dati personali;
b. Il Piano per la gestione delle violazioni di dati personali di competenza;
c. Il Piano di attuazione delle politiche di sicurezza relative ai trattamenti informatici/digitali di dati personali, in conformità delle line guida del RDP e dell'Agenzia per l'Italia Digitale;
d. Un Piano di supporto all'attività delle strutture di ASSA S.P.A. nell'applicazione delle politiche di sicurezza informatica, anche attraverso l'identificazione di specifiche soluzioni tecniche e procedurali e l'individuazione delle misure di protezione adeguate al rischio;
e. Le misure di tenuta della documentazione relativa alle misure di sicurezza applicate alle infrastrutture e alle applicazioni gestite e degli esiti degli eventuali controlli di vulnerabilità effettuati, salvo che tale compito sia stato affidato a un fornitore designato responsabile del trattamento;
f. L'elenco aggiornato e la pubblicazione dell'elenco delle banche dati informatiche come previsto dal CAD;
g. L'elenco designazione amministratori di sistema e amministratori di singole postazioni di lavoro nei limiti concordati con il titolare e il RPD in conformità ai provvedimenti generali del Garante dei dati personali;
h. Le attività previste nel Piano di gestione delle violazioni di dati personali (Data Breach) e delle attività necessarie per l'applicazione della metodologia di analisi dei rischi o per l'eventuale valutazioni di impatto sulla protezione dei dati, sia sui trattamenti già in corso, sia all'avvio di nuovi trattamenti con strumenti informatici o dell'utilizzo di nuovo tecnologie, in conformità ai principi della protezione dei dati fin dalla progettazione (privacy by design) e della protezione per impostazione predefinita (privacy by default).
4.Il dirigente, ovvero la P.O. o il dipendente dell'Ufficio ICT svolge i compiti e le funzioni raccordandosi con il RPD con il titolare, o suo delegato, con il Responsabile per la Transizione al digitale è con gli altri component del Gruppo di lavoro privacy.

Art. 13 Gruppo di lavoro e referente privacy

1.Il Referente Privacy è un dipendente di ASSA S.P.A. che coadiuva il Titolare nell'espletamento dei molteplici compiti afferenti la tematica dei dati personali svolti dall'Ufficio e per il Direttore Generale si interfaccia con il Responsabile per la Protezione Dati e al quale assicura i mezzi necessari per lo svolgimento delle attività, ne condivide l'Agenda delle riunioni alle quali il RPD deve necessariamente essere presente quando vengono adottati procedimenti innovativi o innovazione tecnologiche ed organizzative dell'Ente.

Art. 14 Responsabile della Protezione dei dati

1.Il RPD ha in ASSA S.P.A. un ruolo fondamentale per la promozione della cultura della protezione dei dati e per l'attuazione del GDPR e dei principi fondamentali del trattamento; i diritti degli interessati; la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita; i registri delle attività di trattamento; la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali; le misure tecniche; la modulistica la consulenza legale in materia di privacy e protezione dei dati.
2. In ottemperanza all'art. 39 comma 1 del Reg. UE 2016/679 il DPO è incaricato di:
a. informare e fornire consulenza al titolare del trattamento e ai responsabili del trattamento, ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dall'applicazione della normativa;
b. sorvegliare sull'attuazione in ASSA S.P.A. delle disposizioni del Regolamento UE sulla protezione dei dati, le disposizioni degli Stati membri relativamente alla protezione dei dati, delle politiche del titolare in materia di protezione dei dati personali, la formazione del personale, le attività di controllo;
c. cooperare con l'autorità di controllo, ne è il referente e fungere da punto di contatto per questioni del trattamento, tra cui la consultazione preventiva di cui all'art. 36 del Reg. UE 2016/679;
d. vigilare in ASSA S.P.A. per le attività alla stessa spettante in materia di Registro dei trattamenti. Supporta la revisione delle informative e del consenso per conformarle al GDPR;
e. svolgere attività di consulenza preventiva in materia di protezione dei dati, monitorare e consigliare le politiche di protezione dei dati adeguate alle specifiche attività svolte da ASSA S.P.A., esprimere parere sui contratti tra contitolari e tra titolare e responsabili;
f. fornire supporto al Titolare in ordine alla valutazione d'impatto sulla protezione dei dati e vigila sullo svolgimento ai sensi dell'articolo 35 del Regolamento;

g. svolgere le funzioni comunque assegnate dalla normativa vigente e nell'esecuzione dei compiti il RPD compie una valutazione dei rischi tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo e nella valutazione del "rischio" è titolato a conduce una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment - DPIA);
h. gestire i tentativi e le violazioni dei dati personali (Data Breach) e partecipare alle riunioni del Gruppo di lavoro;
i. monitorare e gestire i reclami sulla base della procedura fissata nel presente regolamento, partecipare alla redazione dei codici di condotta ed esprime parere sulle certificazioni.
3. Il conferimento dell'incarico al RPD è fatto con atto Aziendale ai sensi dell'art. 5 lett. l. del presente regolamento, sulla base dell'art. 7, comma 6, D.lgs. 165/2001, previa procedura selettiva comparativa.
4. Il nominativo deve essere immediatamente comunicato all'Autorità di controllo e il RPD entra nelle funzioni con la sottoscrizione del contratto.

Art. 15 Trattamento dei dati nell'ambito del rapporto di lavoro pubblico

1. Per i trattamenti nell'ambito del rapporto di lavoro pubblico si rinvia all' art.111 del D. Lgs. 196/2003 che prevede l'adozione di Regole deontologiche che saranno approvate dal garante ai sensi dell'articolo 2-quater del Codice Privacy, per i trattamenti dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendosi anche specifiche modalità per le informazioni da rendere all'interessato.
2. ASSA S.P.A. può comunicare ad altre amministrazioni pubbliche i dati trattati quando la comunicazione dei dati ha base nella legge o deve essere effettuata in esecuzione di compiti di interesse pubblico ai sensi dell'art. 2 sexies del D. Lgs. 196/2003 ovvero nell'esercizio del pubblico potere attribuito e per gli obblighi previsti e volti a tutelare le esigenze della legislazione fiscale, assistenziale e previdenziale.
3. La comunicazione dei dati a terzi è consentita in forma anonima e ai fini delle politiche del lavoro e di statistica ricavati dalle informazioni relative a singoli o a gruppi di lavoratori: come il numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate nelle varie articolazioni organizzative, gli importi di trattamenti stipendiali o accessori individuati per fasce o qualifiche/livelli professionali, le giornate non lavorato per motivi di salute, o per benefici di legge anche nell'ambito di singole funzioni o unità organizzative, salvo che anche tale diffusione di dati anonimi sia di pregiudizio per la libertà e dignità del lavoratore qualora individuabile.
4. Ad esclusione dei casi in cui il contratto collettivo applicabile preveda espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale per verificare la corretta attuazione di taluni atti organizzativi, l'amministrazione può fornire alle organizzazioni sindacali dati numerici o aggregati e non anche quelli riferibili ad uno o più lavoratori individuabili. È il caso, ad esempio, delle informazioni

inerenti ai sistemi di valutazione dell'attività dei dirigenti, alla ripartizione delle ore di straordinario e alle relative prestazioni, nonché all'erogazione dei trattamenti accessori.
5. L'amministrazione può anche rendere note alle organizzazioni sindacali informazioni personali relative alle ritenute effettuate a carico dei relativi iscritti, in conformità alle pertinenti disposizioni del contratto applicabile.

Art. 16 Dati relativi ai concorsi e alle selezioni pubbliche

1. Il trattamento dei dati relativi a concorsi pubblici è consentito presso ASSA S.P.A. in conformità del parere del Garante Privacy del 2014. Quando la selezione contiene parametri, ai fini del posizionamento in graduatoria, che direttamente o indirettamente siano idonei a recare pregiudizio alla libertà e alla dignità dei concorrenti i nominativi degli stessi dovranno essere trattati e pubblicati in forma anonima.
2. L'Ente, nel rispetto della previsione di cui al precedente co.1, può lecitamente trattare, in base a specifiche previsioni legislative o regolamentari, solo i dati personali pertinenti e non eccedenti ai fini del corretto espletamento della procedura concorsuale e della sua rispondenza ai parametri stabiliti nel bando e applicando, nella pubblicazione, i principi della minimizzazione e anonimizzazione dei dati (elenchi nominativi resi anonimi e per codice ai quali vengano abbinati i risultati di prove intermedie, elenchi degli ammessi alle prove scritte o orali, punteggi riferiti a singoli argomenti di esame; punteggi totali ottenuti).
3. Le informazioni di cui all'articolo 13 del Regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento UE 679/2016 e il consenso al trattamento dei dati personali presenti nei curricula non è dovuto e il curriculum potrà essere pubblicato salvo che, previa resa informativa, l'interessato autorizzi espressamente la pubblicazione.

Art. 17 Trattamenti basati sul consenso dell'interessato

1. Qualora il trattamento sia basato sul consenso l'Ente deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali in relazione alla finalità specifica per le quali lo ha reso. Il consenso può essere dato oralmente o per iscritto, anche attraverso mezzi elettronici ma deve essere espresso in forma comprensibile chiaro ed inequivocabile.

2. Quando l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali può essere effettuato solo per la finalità specifica per la quale è stato reso.
3. Il consenso reso per uno dei trattamenti di cui all'art. 9 del GDPR 679/2016 è sempre revocabile salvo che il diritto dell'Unione o degli Stati membri disponga espressamente che l'interessato non possa revocare il consenso reso.
4. L'interessato ha, per i dati diversi di cui all'art. 9 del GDPR, il diritto di revocare il proprio consenso in qualsiasi momento, la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca, ma legittimamente comporta che laddove il servizio non posso essere più reso, perché il trattamento è essenziale per il servizio reso lo stesso non sarà più reso, previa idonea informativa all'interessato revocante.
3.Per le pubbliche amministrazioni la base normativa sostituisce il presupposto del consenso, pertanto i soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati persona.

Art. 18 Diritti degli interessati riconosciuti dall'Ente

1.Gli interessati esercitano i loro diritti facendo ricorso alla modulistica pubblicata sul sito dell'Ente e nel rispetto delle norme previste nel Codice per l'esercizio dei diritti dell'interessato pure pubblicato sul sito istituzionale dell'Ente.
2.Il Diritto di accesso dell'interessato ex art. 15 del Regolamento UE 2016/679 si sostanzia nel diritto dell'interessato di ottenere dal titolare conferma che sia o meno in corso un trattamento dei propri dati personali e, in tal caso, l'accesso alle informazioni espressamente previste dall'articolo citato, tra cui a titolo esemplificativo e non esaustivo le finalità del trattamento, le categorie di dati e destinatari, il periodo di conservazione, l'esistenza del diritto di cancellazione, rettifica o limitazione, il diritto di proporre reclamo, tutte le informazioni disponibili sull'origine dei dati, l'eventuale esistenza di un processo decisionale automatizzato ai sensi dell'art. 22 del Regolamento, nonché copia dei propri dati personali.
3. Il Diritto di rettifica ex art. 16 del Regolamento UE si sostanzia nel diritto dell'interessato di ottenere dal titolare la rettifica e/o l'integrazione dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo.
4. Il Diritto alla cancellazione "diritto all'oblio" ex art. 17 del Regolamento UE si sostanzia nel diritto dell'interessato alla cancellazione dei propri dati personali senza ingiustificato ritardo, se sussiste uno dei motivi espressamente previsti, tra cui a titolo esemplificativo e non esaustivo il venir meno della necessità del trattamento rispetto alle finalità, la revoca del consenso su cui si basa il trattamento, opposizione al trattamento nel caso in cui sia basato su interesse

legittimo non prevalente, trattamento illecito dei dati, cancellazione per obblighi di legge, dati dei minori trattati in assenza delle condizioni di applicabilità previsto dall'art. 8 del Regolamento;
5. Il Diritto di limitazione del trattamento, ai sensi dell'art. 18 del Regolamento UE, si sostanzia nel diritto a limitare il trattamento illecito, la contestazione dell'esattezza dei dati, l'opposizione dell'interessato e il venir meno del bisogno trattamento da parte del titolare, i dati dell'interessato devono essere trattati solo per la conservazione salvo il consenso dello stesso.
6. Il Diritto alla portabilità dei dati ex art. 20 del Regolamento UE conferiscono all'interessato, nei casi in cui il trattamento si basi sul consenso e sul contratto e sia effettuato con mezzi automatizzati, potrà richiedere di ricevere i propri dati personali in formato strutturato, di uso e leggibile da dispositivo automatico, e ha diritto di trasmetterli a un altro titolare.
7.Per Diritto di opposizione, ex art. 21 del Regolamento UE, si intende il diritto dell'interessato di opporsi al trattamento dei propri dati personali, nel caso in cui il trattamento sia basato su interesse legittimo.
8. Il Diritto di non essere sottoposto a processi decisionale automatizzato, ex art. 22 del Regolamento UE, si sostanzia per l'interessato a non essere sottoposto ad una decisione, compresa la profilazione, basata unicamente sul trattamento automatizzato.
9.Il diritto all'obblio di ogni individuo si sostanzia nel diritto ad essere dimenticato per fatti che lo riguardano e che in passato sono stati oggetto di cronaca non più di attualità e rispetto ai quali non vi è un interesse pubblico attuale.
10. L'Ente al venire meno dello scopo rispetto al quale i dati sono stati raccolti, l'interessato ha diritto di ottenere dal Titolare la cancellazione dei dati personali. II Titolare dal trattamento ha l'obbligo di cancellare i dati personali resi pubblici, con la tecnologia disponibile, chiedendo la cancellazione di qualsiasi link, copia o riproduzione dei dati medesimi.

Art. 19 Attività di conciliazione pre-reclamo

1. Fatto salvo il diritto di Reclamo al garante privacy o il ricorso in sede giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi i suoi dati personali ha il diritto, ricorrendo alla modulistica ASSA S.P.A., di richiedere al Responsabile alla protezione dei dati, con istanza motivata, le ragioni della ritenuta violazione e che il comportamento ritenuto lesivo sia dismesso da parte dell'Ente.
2. L'esame dell'istanza è orientato a criteri rapidità e di semplicità delle forme osservate, di celerità ed economicità, anche in riferimento al contraddittorio e il pre-reclamo non comporta alcun contributo spese. Al termine dell'istruttoria il RPD concludere l'esame dell'istanza accogliendola o archiviandola.

Art. 20 Entrata in vigore – Pubblicità

1.Il presente Regolamento dopo l'approvazione e sarà pubblicato ed entra in vigore il giorno successivo.

RIV_5/11/2020