REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI E SOCIAL MEDIA POLICY REG. EUROPEO 679/2016

AGENZIA PER IL DIRITTO ALLO STUDIO DELLA REGIONE PUGLIA

(A.DI.S.U. – PUGLIA)

INDICE

1. PREMESSA

Con il presente documento si intende portare a conoscenza di tutto il personale dell'A.DI.S.U. - Puglia un regolamento generale, che regoli e disciplini il trattamento di tutti i dati in materia di privacy.

La progressiva diffusione delle nuove tecnologie informatiche espone il titolare e gli utenti (tra cui dipendenti e collaboratori) a rischi di natura patrimoniale, oltre che alle responsabilità conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi legati alla sicurezza oltre che all'immagine ed all'organizzazione del titolare del trattamento.

Il regolamento si applica a tutti i lavoratori dipendenti, nonché a tutto il personale che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto di lavoro e/o utilizzazione con lo stesso intercorrente - presti la propria attività lavorativa, anche saltuaria e/o consulenziale, presso il titolare del trattamento o che, per ragioni connesse all'espletamento del proprio lavoro, risulti comunque autorizzato e abilitato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il titolare adotta il presente Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i soggetti autorizzati al trattamento dati per conto del Titolare.

Considerato inoltre che, il titolare nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, indirizzi mail, ecc...), sono state inserite nel regolamento alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

Compete all'Agenzia:

a) assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

b) adottare idonee ed adeguate misure di sicurezza per assicurare la riservatezza, la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti ed in generale qualunque accadimento che possa ledere i diritti dei soggetti interessati;

c) tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa.

d) Le informazioni così trattate contengono dati personali, potenzialmente anche sensibili (particolare secondo la definizione del GDPR), riguardanti lavoratori o terzi, "identificati" o "identificabili".

FINALITA':

Scopo del presente Regolamento è quello di organizzare il funzionamento e il corretto impiego degli strumenti elettronici definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto, in particolare:

- dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali;
- della normativa in materia di protezione dei dati personali;
- delle esigenze di tutela della sicurezza della disponibilità e dell'integrità dei sistemi informativi e dei dati, anche al fine di prevenire eventuali usi indebiti degli strumenti elettronici in parola.

Ulteriori finalità del presente Regolamento sono, da un lato, informare i lavoratori ed i collaboratori sulla necessità di effettuare eventuali controlli a tutela della sicurezza della rete informatica e, dall'altro, sensibilizzare il medesimo personale su ulteriori aspetti, non meno rilevanti, relativi alla gestione dei sistemi informativi aziendali e al corretto trattamento dei dati gestiti nella normale attività aziendale.

Riferimenti normativi e regolamentari:

- **GDPR n. 679 del 2016;**
- **D.lgs n. 101 del 2019;**
- **D.lgs n. 196 del 2003;**
- **Circolari del Garante della Protezione dati e s.m.i.;**
- **Statuto dei lavoratori (Legge 300/70 - ART. 4) - *Impianti audiovisivi e altri strumenti di controllo*;**
- **Codice di comportamento A.DI.S.U. Puglia (deliberazione del C.d.A. n. 1 del 31/01/2014) con riferimento all'art. 16 sull'utilizzo delle apparecchiature informatiche.**

2. Definizioni (GDPR)

- **"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;

- **"trattamento":** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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;

- **"limitazione di trattamento":** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento futuro;

- **"profilazione":** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a 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;

- **"pseudonomizzazione":** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti ad 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;

- **"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 e 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 le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- **"responsabile del trattamento":** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- **"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;

- **"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;

- **"consenso dell'interessato":** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazioni o azione positiva inequivocabile, che i dati personali che lo riguardano siano effetto di trattamento;

- **"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;

- **"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;

- **"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 immagine facciale o i dati dattiloscritti;

- **"dati relativi alla salute":** i dati personali attinenti alla salute fisica o montale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute:

- **"stabilimento principale":** a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile de trattamento nella misura

in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

- **"rappresentante":** la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

- **"impresa":** la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

- **"gruppo imprenditoriale":** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

- **"norme vincolanti d'impresa":** le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

- **"autorità di controllo":** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; L 119/34 IT Gazzetta ufficiale dell'Unione europea 4.5.2016

- **"autorità di controllo interessata":** un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

- **"trattamento transfrontaliero":** a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione,

ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

- **"obiezione pertinente e motivata":** un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

- **"servizio della società dell'informazione":** il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

- **"organizzazione internazionale":** un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

- L'Art. 9 del Regolamento UE intende per **"dati particolari (sensibili)"** tutti quei dati personali atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici, i dati relativi alla salute e i dati relativi alla vita sessuale o all'orientamento sessuale della persona.

- L'Art. 10 del Regolamento intende per **"dati giudiziari"** tutti quei dati personali relativi alle condanne penali e ai reati.

3. Utilizzo del Personal Computer

- Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

- La nostra struttura mette a disposizione di tutti gli utenti una stazione di lavoro configurata in modo standard tramite personale dedicato all'attività o al supporto IT che può essere interno o le attività possono essere affidate soggetti terzi che svolgono servizi in relazione a specifico contratto.

- I personal computer ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

- L'infrastruttura tecnologia, anche se solo in uso da parte della nostra organizzazione, è a tutti gli effetti un bene aziendale ivi comprese le informazioni contenute.

- Il personal computer dato in affidamento all'utente permette l'accesso alla rete e ai sistemi solo attraverso specifiche credenziali di autenticazione come meglio descritto successivamente nel presente Regolamento.

- Si rende noto che il personale, interno ed esterno, che opera per garantire la corretta configurazione e funzionamento del sistema informatico (nel seguito per brevità "Servizio IT") è autorizzato a compiere interventi diretti a garantire la funzionalità, la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware ecc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti descritti nei paragrafi 6 e 7, potranno anche comportare l'accesso in caso di effettiva necessità, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività, si applica anche in caso di assenza prolungata o impedimento dell'utente, in caso di effettiva necessità. Si precisa sin da ora che tali azioni saranno poste in essere solo se strettamente necessarie, prediligendo, caso per caso, interventi che non comportano trattamento dati, se non indispensabili.

  (Vedi Appendice A in caso di segnalazione di incidente di sicurezza).

- Il personale incaricato del Servizio IT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso all'utente e si procederà con la sua fattiva collaborazione.

- Salvo preventiva autorizzazione della nostra organizzazione, anche tramite personale del Servizio IT, non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del predetto servizio, né viene consentito agli utenti di installare autonomamente programmi o strumenti provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni esistenti. L'inosservanza della presente disposizione espone l'organizzazione a gravi responsabilità civili o addirittura penali. Si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

- Salvo preventiva autorizzazione dell'organizzazione, anche tramite personale del Servizio IT, non è consentito all'utente di modificare le caratteristiche impostate sul proprio PC o sui sistemi per i quali è stato consentito e configurato l'accesso, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro.

- Il Personal Computer, ed ogni strumento lavorativo, deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Il pc in dotazione agli incaricati è ad ogni modo dotato di una modalità manuale di blocco che evita di lasciare incustodito il pc, obbligando a reintrodurre la password per accedere al pc. Stesse regole devono essere adottate per ogni strumento che permette l'accesso alle informazioni.

4. Gestione ed assegnazione delle credenziali di autenticazione

- Le credenziali di autenticazione, tramite il servizio IT, vengono affidate al nuovo utente, previa formale valutazione, anche in sinergia con il responsabile dell'area alla quale sarà assegnato.

- Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user-id), associato ad una parola chiave (password) riservata, che dovrà essere custodita con la massima diligenza e non divulgata.

- L'utente ha l'obbligo di impostare la parola chiave nel momento in cui accede alla rete ovvero alle risorse informatiche.

  Le credenziali di accesso ai vari software in uso dell'A.DI.S.U. - Puglia dovranno rispettare almeno i seguenti criteri:

  - Numero minimo di caratteri alfanumerici: 8;
  - Scadenza password: massimo 90 gg;
  - La nuova password da impostare non può coincidere con la password da sostituire.

  Dovrà essere cura del dipendente provvedere ad impostare le credenziali di accesso qualora il software non permetta di impostarli automaticamente.

  Tuttavia, la procedura di cambiamento della password è gestita, laddove è possibile, in modo completamente automatizzato dal software.

- La composizione della password deve essere effettuata in modo da non contenere riferimenti facilmente riconducibili all'utente (data di nascita, nome, cognome, etc..).

- La propria password e il nome utente assegnato non dovranno essere rivelati a nessuno e per alcun motivo, a meno di nomina di un fiduciario ed/o un custode password che la conserverà in busta chiusa sigillata.

- Non deve essere conservato nessun appunto, e non deve essere inoltrato nessun messaggio (posta elettronica, cartaceo, sms) contenente le credenziali o riferimenti alla stessa, per evitare che altri ne vengano anche accidentalmente a conoscenza.

- Nel caso di sospetto che altri siano a conoscenza della propria password si dovrà modificare immediatamente le proprie credenziali e informare senza indugio il proprio superiore gerarchico.

- Il soggetto preposto al rilascio delle credenziali di autenticazione è il personale incaricato del Servizio IT appositamente nominato.

5. Utilizzo della rete

- Per l'accesso alla rete ciascun utente deve essere in possesso della specifica credenziale di autenticazione;
- È assolutamente proibito appropriarsi di credenziali che non siano state assegnate all'utente tramite un ordine scritto. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e personali e vanno comunicate e gestite secondo le procedure impartite.
- Le cartelle utenti presenti nei server/sul sistema informativo del titolare sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste cartelle. Su queste cartelle vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale del Servizio IT. Le cartelle relative allo spazio cloud a disposizione degli utenti sono soggette a salvataggio automatizzato.
- Il personale del Servizio IT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete, dandone comunicazione all'utente che ne ha effettuato la creazione e/o l'inserimento.
- Gli utenti non possono collegare alla rete del titolare personal computer, notebook, palmari o simili, provenienti dall'esterno, senza aver precedentemente ricevuto esplicita autorizzazione.
- L'utilizzo della rete da parte di ospiti è consentito in modo libero, tuttavia, il medesimo accesso è limitato da vincoli di firewall e con velocità di navigazione limitata.

6. Utilizzo e conservazione dei supporti rimovibili

- Tutti i supporti rimovibili, contenenti dati, con particolare attenzione ai dati particolari e giudiziari, nonché informazioni costituenti *know-how* del titolare, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

- Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il titolare e seguire le istruzioni da questo impartite anche tramite il servizio IT.

- In ogni caso, i supporti contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti attraverso un sistema di criptazione e/o in armadi o cassetti chiusi a chiave.

- È vietato l'utilizzo di supporti rimovibili personali senza esplicita autorizzazione.

- L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

7. Utilizzo di PC portatili

- L'utente è responsabile del PC portatile assegnato e deve custodirlo con diligenza sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.

- I PC portatili utilizzati all'esterno (convegni, visite in azienda ecc...), in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni e di regola devono essere o custoditi sottochiave o portati con sé.

- L'utente dovrà collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento Antivirus e le normali attività di manutenzione.

- È vietato utilizzare abbonamenti Internet privati per collegarsi alla rete.

- Il disco di sistema e il disco dati (nel caso in cui non sia partizione secondaria dell'unico disco presente) dei computer portatili assegnati agli incaricati sono protetti da crittografia locale impostata, prima della consegna, dal personale del Servizio IT che custodirà anche le chiavi private per la decodifica.

8. Uso della posta elettronica

- La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

- L'abilitazione della posta elettronica è autorizzata dalla nostra organizzazione, che definisce anche il riferimento alla stessa che potrà contenere sia indicazioni dell'utilizzatore che del ruolo secondo necessità (ad esempio <iniziale del nome>.<cognome>@adisupuglia.it).

    - È fatto divieto di utilizzare le caselle di posta elettronica a dominio del Titolare del trattamento (anche se contenenti nome e/o cognome) per motivi diversi da quelli strettamente legati all'attività lavorativa, in quanto la casella di posta elettronica non viene assegnata per uso personale.

- Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenente impegni contrattuali o precontrattuali per il titolare ovvero contenente documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere rigirata all'ufficio competente.

- È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

- È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web sconosciuti).

- Al fine di garantire la funzionalità del servizio di posta elettronica, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) potrà essere impostato per inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto dell'Agenzia. In tal caso, la funzionalità deve essere attivata dall'utente.

- In caso di assenza non programmata (ad es. per malattia) la procedura descritta nel punto precedente, non potendo essere attivata dal lavoratore, verrà attivata dal responsabile del servizio o del settore tramite il servizio IT.

- Il responsabile di settore o di servizio, anche tramite incaricati del Servizio IT, potrà accedere alla casella di posta elettronica per le sole finalità relative al corretto svolgimento delle attività e funzioni lavorative, dandone in tali casi riscontro all'interessato.

- Al fine di ribadire agli interlocutori la natura esclusivamente professionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato (fornito dal titolare), che non dovrà essere disattivato dall'utente, nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato dal titolare potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella policy del titolare.

- Applicativi, firme elettroniche, e-mail o PEC: devono essere adoperate solo dal proprietario che detiene i codici per il suo utilizzo. Oppure l'uso è consentito solo a persona debitamente delegata per iscritto a tale attività dal proprietario; la delega deve specificare quali siano gli utilizzi consentiti.

- In caso di cessazione del rapporto di lavoro la password di accesso all'indirizzo di posta elettronica assegnata verrà modificata, proibendone in tal modo l'accesso all'ex dipendente.

- In caso di cessazione del rapporto di lavoro, oltre alla disattivazione della casella mail, si procederà ad impostare un sistema di risposta agli eventuali terzi che dovessero inviare messaggi allo specifico indirizzo. Tali risposte conterranno indicazioni concernenti altre forme di contatto del titolare del trattamento.

- La trasmissione all'interno dell'Agenzia di file contenenti dati personali definiti particolari (stato di salute, dati sanitari, disabilità, L. 104/92 ecc…) o dati giudiziari, ai sensi degli artt. 9 e 10 del GDPR 679/2016, dovrà avvenire con la massima attenzione e cautela in ordine all'importanza e alla delicatezza degli stessi. Resta inteso che, in caso di eventuale trasmissione a terzi non destinatari di dati particolari e/o giudiziari, deve essere immediatamente coinvolto il responsabile della protezione dati (DPO) e si devono attendere opportune istruzioni.

9. Navigazione Internet

- Il PC assegnato al singolo utente ed abilitato alla navigazione Internet costituisce uno strumento di lavoro utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

- In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per:

  - l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e/o musica) e previa verifica dell'attendibilità dei siti in questione (in caso di dubbio, dovrà essere a tal fine contattato il personale del Servizio IT);

  - l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal titolare;

  - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

  - la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati;

  - accessi a connessioni anonime o connessioni cifrate che, non permettono l'identificazione dell'indirizzo di navigazione, o comunque a connessioni non autorizzate dal sistema.

- Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il titolare rende peraltro nota l'adozione, anche tramite il servizio IT, di uno specifico sistema di blocco o filtro automatico che prevenga determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black-list.

- Gli eventuali controlli, compiuti dal personale incaricato del Servizio IT, potranno avvenire anche attraverso sistemi quali ad esempio firewall, che consente la

creazione di black-list, blocchi e filtri, e mediante verifica dei file log presenti sui singoli pc client, sempre per la verifica di condotte illecite o anomalie di sistema. Il trattamento sarà svolto in forma automatizzata e/o manuale, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza, ad opera di soggetti a ciò appositamente autorizzati, in ottemperanza a quanto previsto dal regolamento europeo GDPR 679/16. Sarà facoltà del Titolare, tramite il servizio IT, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici lavorativi e ai documenti ivi contenuti, solo in caso di necessità.

- Gli eventuali controlli, compiuti dal personale autorizzato, potranno avvenire mediante sistemi in grado di verificare in particolare i tempi di navigazione e il numero di accessi ad Internet.

- Il controllo con i sistemi sopra descritti non è continuativo, ma viene posto in essere solo in caso si riscontrassero anomalie e verrà effettuato inizialmente sulla base di informazioni anonime ed aggregate, intervenendo in modo più invasivo solo qualora circostanze oggettive e documentate ne giustificassero la necessità. Tali attività, come tutte le azioni di trattamento, saranno effettuate solo da soggetti appositamente incaricati; i file stessi vengono conservati per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del titolare. Sarà in ogni caso seguito il principio di pertinenza temporale del trattamento, in modo che la tenuta dei dati sia effettivamente congrua e giustificabile alla luce delle esigenze tecniche di gestione del sistema informatico.

10. Social Media Policy

- Il titolare, vista l'enorme diffusione dei Social Network a livello globale e considerati i molteplici e rilevanti rischi che questi nuovi canali di comunicazione introducono, ne vieta tassativamente l'uso attraverso i dispositivi aziendali. La tutela delle informazioni assume un ruolo di fondamentale importanza, tale da non poter essere messa a rischio; per questo motivo, con il presente Regolamento il titolare ha altresì ritenuto di fornire al proprio personale alcune indicazioni dirette a guidare un utilizzo responsabile dei social media anche a livello personale;

- È vietato l'utilizzo dei social network durante l'orario di lavoro, durante l'espletamento di qualsiasi servizio, e nei confini della sede stessa del titolare. Solo il personale espressamente autorizzato con formale lettera di incarico e nomina, in ragione della

specifica mansione lavorativa ricoperta, potrà utilizzare i social network durante l'orario di lavoro;

- Quando ci si esprime nei social media, è essenziale ricordare sempre che si è responsabili delle proprie comunicazioni;
- Non pubblicare contenuti o materiali coperti da riservatezza o segreto;
- Non pubblicare materiali o contenuti offensivi, illegali, vessatori, diffamanti, minacciosi, volgari, osceni, che ledano diritti di terzi e/o che incoraggino condotte contrarie alle vigenti normative, ai codici di condotta o simili;
- Se ci si imbatte in commenti sul conto dell'Agenzia:
  - Se i commenti sono positivi: interagire liberamente, ma nel pieno rispetto delle regole qui sopra elencate;
  - Se i commenti sono negativi: astenersi dall'interagire e contattare il superiore gerarchico per renderlo edotto sui fatti;
  - Se i commenti hanno ad oggetto argomenti che richiedono competenze specifiche: astenersi dall'interagire e contattare il superiore gerarchico per renderlo edotto sui fatti;
  - In caso di dubbi, astenersi dall'interagire e contattare il proprio superiore gerarchico per renderlo edotto sui fatti.

11. Protezione antivirus

- Il sistema informatico dell'A.DI.S.U. – Puglia è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico.
- Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà prontamente segnalare l'accaduto al servizio IT, in caso di assenza l'utente dovrà spegnere il pc.
- Ogni dispositivo magnetico esterno al computer (pen-drive, hard disk ecc…) dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, non dovrà essere utilizzato (si ricorda che per l'utilizzo di

dispositivi esterni non forniti dal Titolare è necessario essere preventivamente autorizzati).

12. Utilizzo di telefoni fissi, Smartphones, Mobile Devices ed equiparati, fax e fotocopiatrici aziendali

- Il telefono affidato all'utente è uno strumento di lavoro, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.

- Qualora venisse assegnato uno Smartphone, Mobile Devices ed equiparati all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono: in particolare, salvo esplicita autorizzazione, è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere telefonate/SMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, ivi compreso il salvataggio di immagini, informazioni, messaggi e l'installazione di app o software non autorizzati. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare è possibile soltanto in presenza di preventiva autorizzazione scritta ed in conformità alle istruzioni che saranno fornite al riguardo.

- È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile d'ufficio.

- È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione.

13. Osservanza delle disposizioni in materia di Privacy

- È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure di sicurezza, come indicato anche nella lettera di designazione "persona autorizzata al trattamento" dei dati ai sensi del nuovo regolamento Europeo GDPR 679/16.
  (Vedi Appendice D – Persona autorizzata al trattamento)

14. Accesso ai dati trattati dall'utente

- Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc…) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, ecc…), comunque estranei a finalità di controllo dell'attività lavorativa, è facoltà del titolare, tramite personale appositamente incaricato o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali ed ai documenti ivi contenuti, nonché mediante sistemi tecnologici e/o fatturazione del traffico telefonico e/o dati.

15. Sistemi tecnologici e controlli

- L'Agenzia, preso atto del divieto di utilizzo di strumenti tecnologici preordinati al controllo dell'attività lavorativa del dipendente, assicura che i predetti strumenti tecnologici saranno installati, se del caso, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e/o per la tutela del patrimonio, e per tutte le finalità previste dal rapporto di lavoro e previa idonea informativa all'interessato ed ove necessario tramite autorizzazione dell'ispettorato del lavoro o accordo sindacale.

- Si rammenta che i sistemi informativi per loro natura generano dei Log di regola aggregati ed anonimi durante l'utilizzo dei sistemi stessi. Tali strumenti, essendo tecnicamente indispensabili per il funzionamento dei sistemi informativi fanno parte degli strumenti necessari al lavoratore per compiere la propria prestazione lavorativa,

e pertanto non necessitano di accordi sindacali o autorizzazioni da parte dell'ispettorato.

- Eventuali controlli, che in nessun caso saranno prolungati, costanti o indiscriminati, potranno avvenire secondo le seguenti indicazioni:

  - **Controllo difensivo**: in presenza di seri indizi, il personale appositamente incaricato potrà effettuare, attraverso i predetti sistemi tecnologici, controlli rivolti ad accertare condotte illecite del lavoratore (c.d. controllo difensivo dell'Agenzia), anche mediante verifica dei file log presenti sui singoli pc client, qualora con dette modalità non si pregiudichi la sicurezza del sistema e del trattamento dati;

  - **Controllo graduale**: in caso di anomalie o malfunzionamenti, il personale incaricato effettuerà, mediante l'ausilio dei Sistemi installati, controlli anonimi che si concluderanno con avvisi generalizzati diretti agli incaricati dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie, successive all'invio dell'avviso generalizzato;

  - **Controlli su base individuale** potranno essere effettuati in via eccezionale e tassativa, oltre che nell'ipotesi sopra menzionata, anche ove ricorra una o più delle seguenti ipotesi:

    - quando venga presentata una specifica richiesta di informazioni da parte dell'Autorità giudiziaria;

    - quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato e necessario intervento;

    - I dati raccolti dai predetti controlli potranno essere utilizzati per tutte le finalità connesse al rapporto di lavoro, nel rispetto della normativa sulla privacy e dello statuto dei lavoratori vigente.

      (Vedi Appendice B - Comunicazione della Violazione dei Dati personali (Data Breach) ai soggetti interessati)

16. Amministrazione trasparente

❖ **Procedimenti di accesso civico, generalizzato e documentale.**

1. Il Responsabile della protezione dei dati personali e il Responsabile per la prevenzione della corruzione e della trasparenza, coordinano la loro attività al fine di semplificare e minimizzare l'impatto degli adempimenti sull'attività degli uffici e garantire la massima protezione dei dati personali ogniqualvolta procedimenti di ufficio o attivati su istanza di soggetti esterni, comportino attività di pubblicazione dei dati personali nella sezione "amministrazione trasparente" del sito Istituzionale, ovvero in caso di rilascio di dati personali in occasione di istanze di accesso civico, generalizzato e documentale.

2. In tali ultime ipotesi dovranno essere adottate misure di sicurezza adeguate compresa la pseudonomizzazione, la minimizzazione e la cifratura dei dati personali.

❖ **Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.**

1. Il Responsabile del procedimento o il Servizio/Ufficio che detiene il dato/documento oggetto di pubblicazione nella Sez. "*Amministrazione trasparente*" del sito istituzionale ai sensi del D.lgs. n. 33/2013 e s.m.i., assicura le necessarie misure tecniche ed organizzative affinché, i dati personali contenuti in atti e provvedimenti amministrativi, rispettino i seguenti principi:

a) sicurezza;

b) completezza;

c) esattezza;

d) accessibilità;

e) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.

2. I documenti di cui al comma 1 sono pubblicati, nei termini indicati nel P.T.P.C. dell'Agenzia, sul sito istituzionale dell'amministrazione sez. "*Amministrazione trasparente*" e costantemente aggiornati.

3. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.

4. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza.

5. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.

6. I dati vanno pubblicati in formato di tipo aperto ai sensi dell'art. 68, D.lgs. n. 82/2005 e sono liberamente riutilizzabili secondo la normativa vigente. I dati personali diversi dai dati sensibili e dai dati giudiziari, possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web.

7. I dati, le informazioni e i documenti di cui al comma 1, sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione.

8. Deroghe alla predetta durata temporale quinquennale sono previste:

a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;

b) per alcuni dati e informazioni riguardanti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale ai sensi dell'art. 14, comma 2, D.lgs. n. 33/2013 e i titolari di incarichi dirigenziali e di collaborazione o consulenza, che devono rimanere pubblicati online per tre anni consecutivi a decorrere dalla cessazione del mandato o dell'incarico ai sensi dell'art. 15, comma 4, D.lgs. n. 33/2013;

c) nel caso in cui siano previsti diversi termini dalla normativa in materia di trattamento dei dati personali.

9. I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o

successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

10. Non possono essere disposti filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "*Amministrazione trasparente*".

11. Per tutto quanto non previsto nel presente Regolamento, si fa rinvio alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi del 15.04.2014 (GU n. 134 del 12.06.2014).

- **Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali**

1. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati sensibili e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.
2. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
3. Qualora i dati personali contenuti nei documenti non siano pertinenti o siano eccedenti rispetto all'interesse manifestato dal richiedente nell'istanza di ostensione, al fine di salvaguardare la riservatezza di terzi, l'accesso agli atti può essere limitato, su valutazione del Responsabile del procedimento o del RPCT per quanto all'accesso civico, mediante l'occultamento di alcuni contenuti.
4. Per quanto non indicato nel presente Regolamento, si fa rinvio alle Linee guida dell'ANAC in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali (Delib. n. 1309 del 28.12.2016).

17. Albo pretorio online

1. L'Albo pretorio online assolve all'obbligo della pubblicità legale ai sensi dell'art. 32 della Legge n. 69/2019.
2. L'Agenzia prima di procedere alla pubblicazione degli atti e dei provvedimenti deve compiere una selezione attenta dei dati personali da diffondere, tenuto conto non solo dei principi di pertinenza, non eccedenza e indispensabilità delle finalità perseguite dai singoli atti, ma anche del divieto di diffusione di determinati dati personali e dei dati particolari.
3. Restano a carico del Responsabile del procedimento, tutte le operazioni necessarie a far sì che gli atti pubblicati non violino alcun aspetto della normativa vigente in merito al trattamento dei dati personali, nel rispetto delle disposizioni del Codice in materia di dati personali (GDPR 679/2016 e D. Lgs. 101/2018 e D. Lgs. 30 giugno 2003, n. 196 e s.m.i.) e delle Linee guida del Garante per la protezione dei dati personali in materia di trattamento di dati personali contenuti in atti e documenti amministrativi effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web.

18. Sanzioni

- È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate sono perseguibili nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dalla vigente disposizione di legge applicato dal titolare, nonché con tutte le azioni civili e penali consentite.

19. Aggiornamento e revisione

- Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate e ove si riscontrasse effettiva utilità accolte.

- Il presente Regolamento è soggetto a revisione periodica, almeno annuale, da parte del Responsabile della Protezione Dati dell'A.DI.S.U. - Puglia, ovvero in caso di modifiche dei processi e delle policy da parte titolare.

20. Entrata in vigore del regolamento e pubblicità

- Il presente regolamento entrerà in vigore a partire dalla data di approvazione da parte del C.d.A. dell'Agenzia.

- Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

- Il regolamento verrà comunicato al personale dipendente e pubblicato in modo permanente sul sito istituzionale Amministrazione Trasparente.

21. Campo di applicazione del regolamento

- Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del titolare a prescindere dal rapporto contrattuale intrattenuto con l'ADISU Puglia (lavoratori somministrati, collaboratore a progetto, in stage, ecc…).

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" ed "incaricato" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc…) in possesso di specifiche credenziali di autenticazione. Tale figura sarà indicata quale "persona autorizzata al trattamento".

(Vedi Appendice C – Informativa generale da includere nei bandi di gara: "*INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI RESA AI SENSI DELL'ART. 13 DEL REGOLAMENTO UE N. 679/2016 E D. LGS N. 101/2018 E S.M.I.*"

Appendice A

A.DI.S.U. - PUGLIA	
	Segnalazione incidente di sicurezza

Segnalato a Titolare/ DPO / Responsabile	***Data***
INCIDENTE n. **……..**	
	Rilevazione e Valutazione della Violazione dei Dati personali (Data Breach)

Titolare del trattamento

Denominazione				
Indirizzo	*Prov:*	*BARI*	*nome ente*	*A.DI.S.U. – PUGLIA*
	Cap	*70125*	*Indirizzo*	*VIA GIUSTINO FORTUNATO N. 4/G*
Persona addetta alla comunicazione	*MICHELE PATRONO*			
Funzione rivestita	*DPO*			
Indirizzo PEC o e-mail per eventuali comunicazioni	*dpo@adisupuglia.it*			
Recapito telefonico	*3466698547*			

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verifica la violazione dei dati?

[ ] Il giorno _____
[ ] Tra il _____ e il _____
[ ] In un tempo non ancora determinato
[ ] E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

a) Tipo di violazione

[ ] Lettura (presumibilmente i dati non sono stati copiati) (Riservatezza)
[ ] Copia (i dati sono ancora presenti sui sistemi del titolare)
[ ] Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
[ ] Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
[ ] Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
[ ] Altro:

b) Dispositivo oggetto della violazione

[ ] Postazione di lavoro / computer
[ ] Rete
[ ] Dispositivo mobile
[ ] File o parte di un file
[ ] Strumento di backup
[ ] Documento cartaceo
[ ] Altro:

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

Quali categorie di interessati ha riguardato la violazione di dati?

[ ] Dipendenti
[ ] Minori/Genitori
[ ] Portatori di interesse (stakeolders)
[ ] Altro specificare: ……
[ ] Altro specificare: ……

Quante persone sono state colpite dalla violazione di dati?

[ ] Nr. _____ di persone
[ ] Circa _____ persone
[ ] Un numero (ancora) sconosciuto di persone

Quante registrazioni sono state interessate dalla violazione di dati?

[ ] Nr. _____ di registrazioni
[ ] Circa _____ registrazioni
[ ] Un numero (ancora) indeterminato

Altri dati coinvolti nella violazione

[ ] Dati anagrafici / codice fiscale
[ ] Dati di accesso e di identificazione (user name, password, customer ID, altro)
[ ] Dati relativi a minori
[ ] Dati personali idonei a rivelare lo stato di salute e la vita sessuale
[ ] Dati giudiziari
[ ] Copia per immagine su supporto informatico di documenti analogici
[ ] Ancora sconosciuto
[ ] Altro:

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

[ ] Basso / Trascurabile [ ] Medio [ ] Alto [ ] Molto alto

Misure tecniche ed organizzative applicate ai dati colpiti dalla violazione

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Valutazione dei rischi conseguenti l'evento per i diritti e le libertà degli interessati, tenendo in considerazione le misure preventive attuate per far fronte ai danni

[ ] NON PRESENTI [ ] PRESENTI [ ] ELEVATI

Natura della comunicazione

[ ] Nuova comunicazione
[ ] Inserimento ulteriori informazioni sulla precedente comunicazione (numero di riferimento) _____

La violazione è stata comunicata anche agli interessati?

[ ] Sì, è stata comunicata il _____
[ ] Si sta provvedendo ad effettuare la comunicazione nelle prossime ore
[ ] No, perché _____

La violazione coinvolge interessati che si trovano in altri Paesi UE?

[ ] Sì [ ] No

La comunicazione è stata effettuata alle competenti autorità di controllo?

[ ] No, perché _____
[ ] Sì

Appendice B

Comunicazione della Violazione dei Dati personali (Data Breach) ai soggetti interessati

Gentile *interessato*,

l'A.D.I.S.U. - Puglia è molto attenta alla tutela dei dati personali ed attua una serie di misure di sicurezza, tecniche ed organizzative per proteggerli.

Ciononostante, si è verificato un incidente che potrebbe mettere a rischio la sicurezza dei dati che La riguardano e per limitare al massimo gli effetti di questo incidente, stiamo lavorando per contenerne gli effetti.

Al tempo stesso, vogliamo renderti partecipe dell'accaduto e fornirti ogni indicazione possibile nonché alcuni consigli per evitare ulteriori conseguenze.

Le riportiamo di seguito il nominativo del Responsabile Protezione Dati dell'Agenzia che potrà contattare nel caso avesse bisogno di ulteriori informazioni o istruzioni in merito alle azioni che si dovessero rendere necessarie.

Responsabile Protezione Dati (eventualmente da contattare per informazioni sul Data Breach)

Patrono Michele				
	Prov:	BA	Comune	Bari
	Cap	70125	Indirizzo	Via Giustino Fortunato 4/G
Indirizzo e-mail per eventuali comunicazioni	dpo@adisupuglia.it			
Recapito telefonico	346 6698547			

Descrizione della natura della violazione dei dati personali

L'incidente si è verificato:

[ ] Il giorno _____
[ ] Tra il _____ e il _____
[ ] In un tempo non ancora determinato
[ ] E' possibile che sia ancora in corso

Probabili conseguenze della violazione dei dati personali

Quali misure di sicurezza sono state adottate preventivamente o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

Cosa fare per contenere gli effetti della violazione

Restiamo a disposizione per ogni chiarimento si rendesse necessario, rassicurandoti sin d'ora che il Titolare sta già lavorando per risolvere l'increscioso incidente.

Appendice C

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI RESA AI SENSI DELL'ART. 13 DEL REGOLAMENTO UE N. 679/2016 E D. LGS N. 101/2018 E S.M.I.

Ai sensi dell'art. 13 del predetto Regolamento, La informiamo che:

1. I suoi dati personali verranno trattati per le seguenti finalità: svolgimento della procedura selettiva, compreso l'eventuale utilizzo di graduatorie e per il successivo eventuale conferimento del finanziamento di cui al presente Avviso pubblico, per l'esecuzione dei compiti di interesse pubblico o comunque connessi all'esercizio dei pubblici poteri affidati all'A.DI.S.U. - Puglia. I dati saranno trattati per il tempo necessario alla selezione e, in caso di conferimento del suddetto finanziamento, per tutto il periodo in cui intercorre il rapporto instaurato con il titolare del finanziamento e, successivamente alla cessazione, per l'eventuale adempimento di obblighi di legge in conformità alle norme vigenti sulla conservazione degli atti amministrativi.
2. I dati verranno trattati in forma digitale ed analogica, con modalità di organizzazione ed elaborazione correlate alle finalità sopra indicate e, comunque, in modo da garantirne la sicurezza e la riservatezza.
3. Il conferimento dei dati è obbligatorio per l'espletamento della procedura selettiva; l'eventuale rifiuto di fornire tali dati comporta la mancata possibilità di partecipazione alla procedura stessa.
4. Possono venire a conoscenza dei dati in questione, per il conseguimento delle finalità sopra indicate, il Dirigente della Struttura che ha emanato l'avviso di selezione, il responsabile del procedimento, il personale incaricato della gestione delle diverse fasi del procedimento, i componenti della commissione esaminatrice e il segretario.
5. Il Titolare del trattamento è A.DI.S.U. – Puglia, con sede per la funzione alla via Giustino Fortunato 4/G, 70125 - Bari, reperibile all'indirizzo PEC: direzionegenerale@pec.adisupuglia.it.

6. I dati di contatto del Responsabile della protezione dei dati sono: avv. Michele Patrono, reperibile al seguente indirizzo mail: dpo@adisupuglia.it.
7. La graduatoria finale di merito verrà pubblicata con le modalità indicate nel bando di selezione.
8. Saranno altresì diffusi sul sito web dell'A.D.I.S.U. - Puglia, nella sezione "Amministrazione Trasparente" ai sensi e per gli effetti dell'art. 15 comma 1, del D. Lgs. n. 33/2013, le informazioni riguardo il "soggetto proponente".
9. Al termine della procedura selettiva, nei limiti pertinenti le finalità sopra indicate, i dati del "soggetto proponente" potranno essere comunicati a soggetti terzi, in conformità agli obblighi previsti da leggi, regolamenti, normativa nazionale e comunitaria, nonché da disposizioni impartite da autorità a ciò legittimate da organi di vigilanza e di controllo, ai sensi dell'art. 6 del Reg. UE GDPR 679/2016.
10. In qualità di interessato, il "soggetto proponente" ha il diritto di chiedere al Titolare l'accesso ai dati personali che lo riguardano nonché di esercitare i diritti di cui agli articoli 15 e seguenti del Regolamento (UE) 2016/679, tra cui richiedere la rettifica o la cancellazione degli stessi o la limitazione del trattamento o di opporsi al trattamento presentando apposita istanza al contatto di cui al precedente punto 5 e 6.
11. In qualità di interessato, ricorrendone i presupposti, il "soggetto proponente" può presentare reclamo al Garante per la protezione dei dati personali quale autorità di controllo secondo le procedure previste di cui all'art.15 e ss. del suddetto regolamento GDPR 679/2016.

Per presa visione

_____

Luogo e data

_____, __/__/_____

Appendice D

AGENZIA PER IL DIRITTO ALLO STUDIO DELLA REGIONE PUGLIA

(A.DI.S.U. – PUGLIA)

Atto di nomina ad incaricato Persona fisica autorizzata al trattamento dati

Gent.le _____

La normativa europea Reg.Ue 2016/679, che ha visto la piena applicazione a far data dal 25 maggio 2018, impone precise incombenze per garantire riservatezza integrità e disponibilità dei dati trattati.

Nell'ambito dello svolgimento delle sue funzioni legate all'attività professionale svolta nel seguente ambito amministrativo della suddetta Agenzia, Lei viene necessariamente a conoscenza dei contenuti di dati personali trattati sia su basi cartacee che tramite strumenti informatici ed è soggetto che deve necessariamente svolgere operazioni di trattamento per poter espletare correttamente la propria mansione lavorativa.

Con la presente La nominiamo, pertanto, incaricato (persona autorizzata) al trattamento delle seguenti tipologie di dati:

- dati personali ed identificativi (tutte le informazioni che permettano l'identificazione del soggetto cui si riferiscono es. dati anagrafici, recapiti telefonici, fotografie, codici identificativi, ecc…);
- dati particolari (origine razziale o etnica, appartenenza sindacale, dati relativi alla salute);
- dati giudiziari.

Si ricorda che per trattamento è da considerarsi qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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.

Nello specifico, ferma restando la preventiva configurazione degli strumenti aziendali, avrà accesso agli strumenti e potrà trattare i dati contenuti in:

- Posta elettronica
- Navigazione Internet
- Pacchetto Office Microsoft
- Accesso alle cartelle elettroniche presenti su file server
- Accesso alla cartella elettronica assegnata
- Accesso alle stampanti
- Area Intranet dell'Agenzia
- Gestione contratti dipendenti
- Dati fornitori
- Dati studenti
- Dati aggiudicatari di appalto
- Archivio cartaceo del suo ufficio
- File contenente dati personali
- File contenente dati particolari
- File contenente dati giudiziari

Si ricorda che i processi e le procedure di trattamento, ed ulteriori istruzioni possono essere impartite anche con ulteriori documenti ad integrazione della presente nomina.

Le istruzioni, i principi relativi alla gestione dei dati e le misure di sicurezza relative ai trattamenti autorizzati sono indicati nel **nuovo regolamento privacy dell'A.DI.S.U. – Puglia**, a cui tutti gli incaricati dovranno far riferimento.

L'incaricato/persona autorizzata dovrà osservare scrupolosamente tutte le misure di sicurezza già in atto, o che verranno comunicate in seguito dal Titolare o dal Responsabile della Protezione dati.

Titolare del trattamento è: **A.DI.S.U. - PUGLIA**, nella persona del legale rappresentante *pro tempore* Il Direttore Generale dott. Gavino Nuzzo.

Il titolare

Firma per presa visione

_____

Bari, _____