*ALLEGATO B*

Modello per la redazione della Valutazione di impatto (DPIA) ex art. 35 GDPR nel trattamento di dati personali



## Redazione Valutazione di impatto (DPIA) - Informazioni necessarie

Al fine di poter effettuare correttamente la Valutazione di impatto (DPIA) relativa ad uno specifico trattamento, come previsto dall’attuale disciplina sulla protezione dei dati personali (art. 35 GDPR), è necessario fornire le informazioni e la documentazione di seguito riportate.

***NOTA****: I campi contrassegnati con l’asterisco* (\*) *sono obbligatori; l’assenza di uno o più elementi obbligatori potrebbe comportare l’impossibilità di procedere alla gestione della richiesta.*

*In caso di dubbi ovvero di necessità di supporto alla compilazione è possibile contattare direttamente l’Assistenza tecnica del DPO regionale (e-mail assistenzatecnicaprivacy*[*@regione.puglia.it*](mailto:rpd@regione.puglia.it)*) che fornirà tutte le delucidazioni necessarie.*

**Soggetti di riferimento del trattamento (*processo/progetto/intervento/azione*):**

|  |  |  |  |
| --- | --- | --- | --- |
| Ruolo \* | Nominativo \* | E-mail \* | Tel. *(diretto/mobile)* \* |
| Designato \*  *(dirigente competente per materia)* |  |  |  |
| Referenti \*  *(soggetti interni alla Struttura regionale competente per materia, ad es., funzionario, RUP, ecc., incaricato del procedimento/ trattamento dei dati personali)* |  |  |  |

| Definizione del trattamento | |
| --- | --- |
| Denominazione Trattamento Dati Personali \* | *Riportare la denominazione del trattamento (campo Trattamento Dati Personali) così come inserita nell’applicativo software “Registro delle attività di trattamento dei dati” di cui alla DGR 2159/2021 – RAT (*[*https://gdpr.regione.puglia.it*](https://gdpr.regione.puglia.it)*).*  ***[Nota****: Si suggerisce di effettuare un “copia e incolla” del testo dal RAT, al fine di permettere l’identità terminologica propedeutica alla corretta identificazione del trattamento].* |
| Descrizione del trattamento \* | *Riportare una breve descrizione del trattamento, con indicazione del flusso delle informazioni, delle eventuali interconnessioni con altri titolari o della delega ai Responsabili delle attività di trattamento.* |
| Normativa e disposizioni di riferimento \* | *Leggi e Regolamenti regionali, nazionali e comunitari, Atti amministrativi, Direttive, Circolari*  *(tali norme e disposizioni devono essere espressamente richiamate, ed eventualmente allegate alla valutazione:* ***in caso contrario******non si potrà procedere alla redazione della DPIA****).* |

| Motivo di redazione della DPIA | |
| --- | --- |
| Motivo di redazione della DPIA \* | *Specificare le motivazioni di redazione della DPIA:*  La DPIA risulta **obbligatoria** nel caso di risposta affermativa ad **almeno 2 dei seguenti quesiti**, mentre risulta facoltativa nel caso di risposta affermativa ad almeno 1 dei seguenti quesiti (Provvedimento WP-29 n. 248 del 4 ottobre 2017):  I dati personali trattati servono a fare valutazioni o ad assegnare punteggi ?  I dati personali trattati servono a prendere decisioni automatiche ?  I dati personali trattati servono per il monitoraggio sistematico dell’interessato ?  Si trattano dati personali sensibili o dati aventi carattere altamente personale (dati riguardanti la salute, l’orientamento sessuale, le opinioni religiose, politiche o sindacali, le condanne penali o i reati, ecc.) ?  Si trattano dati personali su larga scala, dal punto di vista sia del numero dei soggetti interessati al trattamento che del volume dei dati trattati ?  I dati personali trattati sono frutto di combinazioni di più fonti (ad es. dati derivanti da due o più operazioni di trattamento e/o da titolari del trattamento diversi?  I dati personali trattati riguardano soggetti vulnerabili ?  I dati personali sono trattati per mezzo di nuove tecnologie evolute e/o nuove soluzioni organizzative ?  Il trattamento dei dati personali può impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto ?  *Ai fini di una valutazione approfondita in ordine alla necessità di redazione della DPIA, si richiamano altresì i criteri contenuti nell’Allegato 1 al provvedimento dell’Autorità Garante Privacy (GPDP) n. 467 dell’11 ottobre 2018 [doc. Web n. 9058979], di seguito riportati*:   1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”. 2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi). 3. Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc. 4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti). 5. Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione)dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8). 6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo). 7. Trattamenti effettuati attraverso l’uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 . 8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche. 9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l’incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*). 10. Trattamenti di categorie particolari di dati ai sensi dell’art. 9 GDPR oppure di dati relativi a condanne penali e a reati di cui all’art. 10 GDPR interconnessi con altri dati personali raccolti per finalità diverse. 11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento. 12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento |

| Requisiti minimi \* | | |
| --- | --- | --- |
| Informativa privacy \*  *(artt. 12, 13, 14)* | *Fornire* ***in allegato*** *l’informativa verticalizzata sul trattamento oggetto di DPIA, completa e/o in formato breve (ad esempio, riportata nella modulistica o pubblicata in piattaforma online).* | *Modalità di ostensione prevista*:  sito web istituzionale/tematico;  piattaforma online dedicata al trattamento;  disponibilità/consegna diretta al singolo interessato;  altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| Nomina soggetti autorizzati \* | *Tutti i soggetti deputati al trattamento devono essere specificatamente autorizzati.* | *Modalità di autorizzazione*:  nomina singolo soggetto autorizzato;  nomina funzionale per appartenenza alla struttura regionale/UO competente. |
| Soggetti coinvolti nel trattamento dei dati personali \* | Titolare: | Regione Puglia |
| Contitolare (eventuale): |  |
| Designati: | Dirigente Struttura \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| Responsabili: | InnovaPuglia S.p.A. |
| *Sub-Responsabili del trattamento (specificare):* |  |
| Nomina Responsabili \* | *I soggetti giuridici che effettuano attività per conto del Titolare del trattamento (fornitori, gestori di servizi, ecc.) devono essere nominati con accordo ai sensi dell’art. 28 GDPR rispetto allo specifico trattamento; tali soggetti, cui devono essere fornite idonee istruzioni relative alle modalità di svolgimento del trattamento, hanno l’obbligo di adottare le misure di sicurezza tecniche e organizzative necessarie rispetto alla tipologia di dati trattati e ai rischi incombenti, unitamente all’obbligo legale di riservatezza del personale impiegato nel trattamento medesimo.* | *Modalità di nomina*:  Contestualmente alla firma del contratto/ convenzione/protocollo d’intesa;  Non sono delegate a soggetti terzi attività di trattamento di dati personali;  Altro (specificare): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| Analisi del  rischio \* | *L’analisi del rischio deve essere effettuata in via propedeutica rispetto alla DPIA – attraverso il “****Modello di Analisi dei Rischi” allegato*** *(All. A) – ed il relativo esito in termini di “LIVELLO DI RISCHIO COMPLESSIVO” deve essere “***ACCETTABILE***”.*  *Nel caso in cui il livello di rischio complessivo risulti* **NON** **ACCETTABILE**,*si dovrà procedere – preliminarmente all’effettuazione della DPIA – con l’adozione di ogni ulteriore misura tecnica e organizzativa prevista dal modello che consenta di arrivare all’accettabilità del rischio [livello di rischio “ACCETTABILE”].*  ***La suddetta analisi del rischio va obbligatoriamente allegata alla DPIA****.* | Risultato dell’Analisi del rischio:  **ACCETTABILE** |

|  |  |  |
| --- | --- | --- |
| Elementi necessari per la valutazione dei rischi \* (*indicare almeno una delle tre tipologie contemplate*) | | |
| Piattaforme informatiche utilizzate nel trattamento | *Riportare gli indirizzi web (URL) delle piattaforme informatiche utilizzate, sia regionali che esterne (ad es., https://<xyz>.regione.puglia.it).* |  |
| Asset utilizzati | *Indicare gli altri applicativi software utilizzati (ad esempio, software installati localmente o condivisioni di rete, file hosting, ecc.).* |  |
| *Indicare i sistemi o dispositivi hardware utilizzati (portatili, tablet, smartphone, IoT, ecc.).* |  |
| Supporti cartacei | *Indicare le modalità di trattamento su supporto cartaceo eventualmente effettuate, inclusa la conservazione.* |  |

Di seguito gli elementi da selezionare o riportare al fine di permettere la corretta redazione della DPIA, verificando sempre l’allineamento con quanto riportato nel RAT per il trattamento in questione:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Valutazione di impatto (DPIA) - Informazioni generali | | | | |
| Tipologia di operazioni effettuate sui dati personali:\* | raccolta | | registrazione | organizzazione |
| conservazione | | adattamento | modifica |
| consultazione | | comunicazione | trasmissione |
| messa a disposizione | | raffronto | interconnessione |
| cancellazione | | distruzione |  |
| Dati personali trattati \* | *Indicare le macrocategorie di dati personali trattati:* | Dati comuni (*nominativo, indirizzo, e-mail, telefono, , ecc.*);  Dati particolari [*art. 9 GDPR*]  Origine razziale o etnica;  Opinioni politiche;  Convinzioni religiose o filosofiche;  Appartenenza sindacale;  Dati genetici;  Dati biometrici;  Dati relativi alla salute;  Dati relativi alla vita sessuale;  Dati relativi all'orientamento sessuale.  Dati soggetti a maggiore tutela dell’anonimato (*relativi ad atti di violenza sessuale o di pedofilia, all’infezioni da HIV o all’uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari*) [“Linee guida in materia di dossier sanitario” - Allegato A alla deliberazione del Garante Privacy del 4 giugno 2015; art. 6, D.M. Ministro della Salute del 7.9.2023 - “Fascicolo Sanitario Elettronico 2.0”];  Dati giudiziari [*art. 10 GDPR*]. | | |
| *Esplicitare la tipologia/ambito di riferimento dei dati personali trattati:* | Famiglia o situazioni personali;  Lavoro (*occupazione attuale e precedente, curriculum, ecc*.);  Istruzione e cultura (*diploma, laurea, attestati, ecc.*);  Documento di riconoscimento;  Documenti reddituali (*dichiarazione dei redditi, buste paga, ecc.*);  Dati patrimoniali reddituali finanziari e assicurativi;  Residenza e recapiti (*indirizzo, mail, telefono, coordinate bancarie, ecc.*);  Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Natura del trattamento | *Indicare eventuali caratteristiche intrinseche del trattamento che possano rappresentare un rischio rilevante per gli interessati*  *[EDPB Guidelines 2019-04 Data protection by design and by default, v. 2.0]:* | Processo decisionale automatizzato;  Rapporti di forza asimmetrici;  Imprevedibilità del trattamento;  Difficoltà per l’interessato di esercitare i propri diritti;  Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Ambito di applicazione | *Indicare la dimensione (potenziale) del trattamento:* | 1 – 1.000 interessati  1.000 – 10.000 interessati  10.000 – 100.000 interessati  Oltre 100.000 interessati  Non definito/definibile | | |
| Materia | *Indicare la materia relativa al trattamento dei dati personali:* | Agricoltura, sviluppo rurale e ambientale  Ambiente, paesaggio e qualità urbana  Bilancio, affari generali ed infrastrutture  Mobilità  Personale e organizzazione  Politiche del lavoro, istruzione e formazione  Promozione della salute e del benessere animale  Sviluppo economico  Turismo, economia della cultura e valorizzazione del territorio  Protezione civile e gestione delle emergenze  Welfare  Gestione e controllo dei fondi europei  Avvocatura regionale  Politiche internazionali  Appalti e contratti  Comunicazione istituzionale  Attività del Gabinetto del Presidente e della Segreteria Generale della Presidenza  Attività della Giunta Regionale  Altro \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Valutazione delle misure atte a garantire necessità e proporzionalità del trattamento  *[art. 35, paragrafo 7, lettera b) GDPR]* | | | | |
| Finalità \* | *Descrivere le finalità del trattamento:* |  | | |
| Condizioni di liceità del trattamento \* | *Indicare la base giuridica ai sensi dell’art. 6 GDPR relativamente ai dati personali comuni :*  *[****in grassetto*** *la base giuridica tipica delle Pubbliche Amministrazioni]* | consenso dell’interessato [*art. 6, par. 1, lett. a) GDPR*] (*da considerarsi del tutto residuale**nell’ambito PA).*  esecuzione di un contratto o di misure precontrattuali [art. *6, par. 1, lett. b) GDPR*];  **obbligo legale [*art. 6, par. 1, lett. c) GDPR*]**;  salvaguardia degli interessi vitali dell’interessato o di un’altra persona fisica [*art. 6, par. 1, lett. d) GDPR*];  **compito di interesse pubblico o connesso all’esercizio di pubblici poteri [*art. 6, par. 1, lett. e) GDPR*]**;  perseguimento del legittimo interesse del titolare del trattamento o di terzi [*art. 6, par. 1, lett. f) GDPR*] (esempio, videosorveglianza); | | |
| *Indicare la base giuridica ai sensi dell’art. 9 GDPR relativamente alle particolari categorie di dati personali (ex dati sensibili), ove trattati:*  *[****in******grassetto*** *la base giuridica tipica delle Pubbliche Amministrazioni]* | consenso dell’interessato [*art. 9, par. 2, lett. a) GDPR*] (*da considerarsi del tutto residuale**nell’ambito PA*);  trattamento necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell’interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale [*art. 9, par. 2, lett. b) GDPR*];  trattamento necessario per tutelare un interesse vitale dell’interessato o di un’altra persona fisica [*art. 9, par. 2, lett. c) GDPR*];  trattamento riguardante dati personali resi manifestamente pubblici dall’interessato [*art. 9, par. 2, lett. e) GDPR*];  trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria [*art. 9, par. 2, lett. f) GDPR*];  **trattamento necessario per motivi di interesse pubblico rilevante [*art. 9, par. 2, lett. g) GDPR*];**  trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali [*art. 9, par. 2, lett. h) GDPR*];  **trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell’assistenza sanitaria e dei medicinali e dei dispositivi medici [*art. 9, par. 2, lett. i) GDPR*];  trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici [*art. 9, par. 2, lett. j) GDPR*]. | | |
| *Indicare la base giuridica ai sensi dell’art. 2-sexies D.lgs. 196/03 relativamente ai dati di natura particolare (sensibili), ove trattati, in caso di trattamenti effettuati per motivi di interesse pubblico rilevante :* | accesso a documenti amministrativi e accesso civico [*art. 2-sexies lett. a) D.lgs. 196/03*];  tenuta di registri pubblici relativi a beni immobili o mobili civico [*art. 2-sexies lett. c) D.lgs. 196/03*];  cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato [*art. 2-sexies lett. e) D.lgs. 196/03*];  elettorato attivo e passivo ed esercizio di altri diritti politici, documentazione delle attività istituzionali di organi pubblici, redazione di verbali e resoconti dell’attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari [*art. 2-sexies lett. f) D.lgs. 196/03*];  esercizio del mandato degli organi rappresentativi, cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche [*art. 2-sexies lett. g) D.lgs. 196/03*];  svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo [*art. 2-sexies lett. h) D.lgs. 196/03*];  attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale [*art. 2-sexies lett. i) D.lgs. 196/03*];  attività di controllo e ispettive [*art. 2-sexies lett. l) D.lgs. 196/03*];  concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni [*art. 2-sexies lett. m) D.lgs. 196/03*];  conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali[*art. 2-sexies lett. n) D.lgs. 196/03*];  rapporti tra i soggetti pubblici e gli enti del terzo settore [*art. 2-sexies lett. o) D.lgs. 196/03*];  attività sanzionatorie e di tutela in sede amministrativa o giudiziaria [*art. 2-sexies lett. q) D.lgs. 196/03*];  rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose [*art. 2-sexies lett. r) D.lgs. 196/03*];  attività socioassistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci [*art. 2-sexies lett. s) D.lgs. 196/03*];  programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale [*art. 2-sexies lett. v) D.lgs. 196/03*];  tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili [*art. 2-sexies lett. aa) D.lgs. 196/03*];  istruzione e formazione in ambito scolastico, professionale, superiore o universitario [*art. 2-sexies lett. bb) D.lgs. 196/03*];  trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan) [*art. 2-sexies lett. cc) D.lgs. 196/03*];  Instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva [*art. 2-sexies lett. dd) D.lgs. 196/03*]. | | |
| Condizioni di liceità del trattamento dei dati giudiziari | *Indicare la base giuridica ai sensi degli artt. 5 e 7 D.lgs. 51/2018 relativamente ai dati di natura giudiziaria di cui all’art. 10 GDPR, ove trattati, in caso di trattamenti effettuati per:* | prevenzione, indagine, accertamento e perseguimento di reati;  esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. | | |
| *Indicare la base giuridica ai sensi dell’art. 2-octies D.lgs. 196/03 relativamente ai dati di natura giudiziaria, ove trattati, in caso di trattamenti effettuati per:* | Adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del GDPR [*art. 2-octies lett. a) D.lgs. 196/03*];  Adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali [*art. 2-octies lett. b) D.lgs. 196/03*];  Verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti [*art. 2-octies lett. c) D.lgs. 196/03*];  Accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia [*art. 2-octies lett. d) D.lgs. 196/03*];  Accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria [*art. 2-octies lett. e) D.lgs. 196/03*];  Esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia [*art. 2-octies lett. f) D.lgs. 196/03*];  Esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza [*art. 2-octies lett. g) D.lgs. 196/03*];  Adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto [*art. 2-octies lett. h) D.lgs. 196/03*];  Accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti [*art. 2-octies lett. i) D.lgs. 196/03*];  Attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese ai sensi dell'articolo 5-ter del decreto-legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla legge 24 marzo 2012, n. 27 [*art. 2-octies lett. l) D.lgs. 196/03*];  Adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo[*art. 2-octies lett. m) D.lgs. 196/03*]. | | |
| Adeguatezza, pertinenza e non eccedenza  (*art. 5, par. 1, lettera c) GDPR*) | *Indicare le misure poste in essere al fine di garantire adeguatezza (efficacia della protezione dei dati):* | sistema di gestione della sicurezza delle informazioni;  analisi del rischio effettuata;  applicati principi di *security/privacy by design;*  verifiche periodiche sui sistemi/piattaforme (VA/PT);  controllo degli accessi (*need to know, need to do*);  limitazione dell’accesso (degli operatori e rispetto ai contenuti);  segregazione dell’accesso;  trasferimenti protetti e sicuri;  conservazione sicura;  pseudonimizzazione;  backup e repliche;  registrazione continua degli eventi e delle azioni (log);  piano di disaster recovery/continuità operativa;  procedura di data breach e risposta agli incidenti. | | |
| *Indicare le misure poste in essere al fine di garantire la pertinenza (correttezza della base giuridica):* | effettuata e mantenuta aggiornata la mappatura dei trattamenti;  applicata la corretta base giuridica, validata con il DPO;  base giuridica differenziata per ciascuna attività di trattamento;  trattamento necessario e non soggetto a condizioni;  piena autonomia dell’interessato nel controllo dei propri dati personali;  base giuridica predeterminata prima dell’inizio del trattamento;  cessazione del trattamento nel caso di base giuridica non più valida;  adeguamento del trattamento rispetto alla eventuale modifica della base giuridica. | | |
| *Indicare le misure poste in essere al fine di garantire la non eccedenza (principio di necessità), anche in logica di privacy by design:* | i dati trattati, le funzioni e i profili di autorizzazione sono predeterminati prima dell’inizio del trattamento;  i dati trattati sono stati minimizzati e validati come nucleo minimo;  sono effettuate verifiche periodiche in relazione ai dati trattati, alle funzioni e ai profili di autorizzazione. | | |
| Esattezza e aggiornamento dei dati  *(art. 5, par. 1, lettera d) GDPR)* | *Indicare eventuali misure poste in essere al fine di garantire esattezza e aggiornamento dei dati.* | fonti dei dati personali affidabili (per dati acquisiti non direttamente dall’interessato);  correttezza dei dati personali verificata periodicamente;  cancellazione/rettifica tempestiva dei dati su richiesta dell’interessato secondo procedura;  effetto della propagazione di errori ridotto grazie ai controlli;  aggiornamento dei dati da parte dell’interessato secondo prevista procedura;  in fase di acquisizione sono previste soltanto scelte concise e predeterminate anziché campi a testo libero. | | |
| Periodo di conservazione dei dati  personali \*  *[NOTA - Occorre compilare obbligatoriamente la prima riga (tempi di conservazione), oppure in alternativa, solo in caso di tempi non definiti, la seconda riga (criteri di determinazione dei tempi)].* | *Indicare le tempistiche previste di conservazione dei dati personali:* | Numero anni: \_\_\_\_\_\_\_\_\_.  *Fonte:*  fonte normativa o amministrativa;  manuale di conservazione documentale regionale;  altro:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. | | |
| *Criteri per determinare il periodo di conservazione, nel caso in cui il numero di anni non sia determinabile con esattezza:* | cancellazione automatica alla conclusione del trattamento;  legato a specifiche necessità e finalità: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;  altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. | | |
| Valutazione delle misure atte a garantire i diritti degli interessati | | | | |
| Esercizio dei diritti | *Indicare le previste modalità di esercizio dei diritti:* | procedura di accesso (art. 15);  procedura di rettifica (art. 16);  procedura di obbligo di notifica (art. 19);  procedura di limitazione e opposizione trattamento (art. 18, 19 e 21). | | |
| Garanzie riguardanti l’eventuale trasferimento dei dati personali in Paesi terzi \*  *(Capo V GDPR)* | *Indicare se sono effettuati trasferimento dei dati personali in Paesi esteri e quali misure sono poste in essere a garanzia dei diritti degli interessati.* | Sono previsti trasferimenti di dati personali fuori dalla UE.  *In caso di trasferimenti extra UE, sono previste le seguenti misura di conformità al trasferimento extra UE:*  decisioni di adeguatezza [*art. 45 GDPR*];  strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici [*art. 46, par. 2, lett. a GDPR*];  norme vincolanti d’impresa [*art. 46, par. 2, lett. b*];  clausole tipo [*art. 46, par. 2, lett. c e lett. d*];  codici di condotta [*art. 46, par. 2, lett. e*];  meccanismi di certificazione [*art. 46, par. 2, lett. f*];  consenso degli interessati (*da considerarsi del tutto residuale**nell’ambito PA).*  *Previa autorizzazione del Garante:*  clausole contrattuali *ad hoc* [*art. 46, par. 3, lett. a*];  accordi amministrativi tra autorità o organismi pubblici [*art. 46, par. 3, lett. b].* | | |
| Consultazione preventiva \*  *(art. 36 GDPR)* | *Riportare se è stata effettuata, anche precedentemente, una consultazione preventiva presso l’Autorità Garante.* | Effettuata consultazione preventiva presso l’Autorità Garante;  non effettuata consultazione preventiva presso l’Autorità Garante. | | |
| Altre informazioni utili alla valutazione |  | | | |
| Opinioni degli interessati o dei loro rappresentanti eventualmente raccolte  *(art. 35, par. 9)* | Non si è ritenuto necessario richiedere parere agli interessati, pur restando fermo l'ascolto di ogni istanza da parte dei loro rappresentanti.  Il parere degli interessati è il seguente: | | | |
| Note |  | | | |

|  |  |
| --- | --- |
| Parere DPO *[spazio riservato al DPO]* | |
| Parere del DPO | **PARERE FAVOREVOLE**  **FAVOREVOLE CONDIZIONATO A**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **PARERE NEGATIVO** |
| Motivazioni del parere |  |