Verbale

“Privacy By design e DPIA”

LZZNDR86D18F205I
/6030032865714004
.yRc9GQow
\+IKcPMitdw/
\+2X8W8Ic\=
Actalis S.p.A.
20.10.2025 08:48:08
GMT+01:00

Servizi integrativi

STEFANO
DANIEL
ANDREA
RUTA
28.10.2025
14:03:22
GMT+00:00

Cronologia delle Revisioni della PRIVACY BY DESIGN e DPIA sulla stessa iniziativa/misura/servizio

Revisione	Data	Sintesi delle Modifiche
1	**09/10/2025**	**Prima emissione**

Indice

1 P1: “ANALISI DEL CONTESTO” 3
2 P2: “FINALITA’ E BASE GIURIDICA” 6
3 P3: “SOGGETTI COINVOLTI” 7
3.1 Soggetti che trattano i dati 7
3.2 Soggetti interessati di cui vengono trattati i dati 7
4 P4: “VALUTAZIONE DI NECESSITA’ E PROPORZIONALITA’” 9
4.1 Dati personali trattati 9
4.2 Operazioni sui dati 11
4.3 Accesso ai dati personali 13
5 P5: “DATA RETENTION” 15
6 P6: “DPIA: QUANDO E PERCHE’” 16
Piattaforma BeS 18
SIUL 22
8 P8: “ADEMPIMENTI PRIVACY” 33
Allegato 1: “ANALISI INTEGRATIVA PER TRATTAMENTI DA SOTTOPORRE A DPIA” 34
1. Valutazioni giuridiche 34
1.1 Valutazioni sul rispetto del principio di trasparenza 34
1.2 Valutazioni sul rispetto del principio di accuratezza 36
1.3 Valutazioni sul rispetto dei diritti e delle libertà fondamentali della persona 37
1.4 Diritti esercitabili dall’interessato 39
1.5 Valutazione dei rischi per i diritti e le libertà degli interessati – rischio informatico 40
1.6 Valutazione giuridica finale sul trattamento 42
2. Valutazioni in materia di sicurezza 44
3. Considerazioni del Titolare del Trattamento 45

1 P1: “ANALISI DEL CONTESTO”

Aspetto	Risposta/Descrizione
Quali sono le **Direzioni di Regione Lombardia** coinvolte?	Direzione generale Istruzione, Formazione, Lavoro
Indicare il **nome dell’iniziativa/misura/servizio**	Servizi integrativi
Fornire una descrizione testuale **dell’iniziativa/misura/servizio.**	La presente misura si pone l’obiettivo di consentire l’**erogazione di una serie di servizi integrativi**, considerati come prestazioni da utilizzare in affiancamento ad una determinata politica attiva per il lavoro. Tali servizi hanno, infatti, lo scopo di rafforzare l'efficacia del programma principale, offrendo **supporti aggiuntivi** che rispondono a **bisogni specifici**. Essi sono fruiti secondo le scelte della persona con disabilità, anche alla luce dell’analisi dei **singoli bisogni** e del **singolo percorso di inserimento lavorativo** che possono riguardare i diversi soggetti con disabilità. I servizi in questione si differenziano in: • **Servizi al lavoro**: i quali includono attività di tutoraggio e potenziamento della rete di supporto e sono finalizzati a facilitare l'integrazione della persona con disabilità in un determinato contesto lavorativo. • **Servizi alla persona**: i quali comprendono attività di supporto più specifiche, come l'assistenza per i bisogni di cura, lo sviluppo dell'autonomia, l'accesso a strumenti professionali e il trasporto.
Indicare la **categoria di dati personali trattati**	☒ Dati personali comuni ☒ Categorie particolari di dati personali ☒ Dati relativi a condanne penali o reati

Quali sono gli **altri soggetti** coinvolti nel trattamento dei dati personali? (fornitori/subfornitori, altre direzioni, altre PA, ecc)	**Responsabili nominati dal titolare** • ARIA S.p.A. • Province e Città metropolitane **Titolari autonomi del trattamento** • Operatori accreditati al lavoro • Datori di lavoro • Altri soggetti che partecipano al Comitato Disabili (L.R. 13/03)
Indicare la **data** (anche approssimativa) di **avvio dell'iniziativa/misura/servizio**	Ottobre 2025
Quali sono le piattaforme informatiche che saranno utilizzate dal servizio informatico? (**esempi di piattaforme informatiche: EDMA, SIAGE, IDPC,**)	- **BeS** - Bandi e Servizi - **SIUL SAP** - **SIUL 68** - **SIUL COB** - **SIUO**
Il trattamento viene effettuato in modalità **cartacea** e/o con l'ausilio di **strumenti informatici**?	L'intero procedimento amministrativo relativo alla misura avviene in modalità telematica.
Vi è un **trasferimento di dati personali al di fuori dello Spazio Economico Europeo**?	No
Ci sono **codici di condotta**, certificazioni di protezione dati o **standard** applicabili al trattamento? (Es: Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali, Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti, Codice di	No

condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica della Regione Veneto, etc.)	

Ciclo di vita del trattamento: descrivere le operazioni di trattamento effettuate, dalla raccolta del dato alla sua cancellazione.

- Gli operatori in possesso di accreditamento per l'erogazione dei **servizi per il lavoro** sono considerati i **soggetti legittimati** a fare domanda per poter accedere al contributo erogato da Regione Lombardia (per dar seguito alla presente misura). Tali enti accreditati presentano, dunque, domanda per conto dei destinatari finali dell'intervento (ossia i soggetti disabili);

- La domanda di contributo viene, pertanto, presentata da parte dei soggetti beneficiari mediante la **piattaforma regionale BeS** (Bandi e Servizi). In tale contesto, andranno inserite le informazioni anagrafiche dell'ente beneficiario e andrà allegato il documento di riconoscimento del rappresentante legale dell'ente in questione (unitamente alla dichiarazione antimafia, ove necessario in ragione dell'importo complessivo richiesto);

- Successivamente alla fase di raccolta delle domande, è prevista una **fase istruttoria,** esperita secondo l'ordine cronologico di presentazione telematica delle domande stesse (e fino ad esaurimento delle risorse finanziarie stanziate). Tale fase istruttoria sarà svolta dalle **Province** e dalle **Città metropolitane competenti**;

- A seguito della **verifica tecnica** relativa alla presenza e alla conformità della documentazione allegata (o a seguito di comunicazione di accettazione da parte del sistema BES), le Provincia e/o le Città metropolitane competenti provvederanno, entro **30 giorni dalla data di presentazione della domanda** di contributo, ad **inviare una comunicazione** contenente il numero del decreto di impegno relativo alla domanda;

- Con riferimento all'erogazione dei servizi integrativi da parte dei soggetti beneficiari, i **funzionari** provinciali e/o i funzionari delle Città metropolitana avranno la facoltà di effettuare, in qualsiasi momento, **opportuni controlli** - anche mediante **ispezioni** e **sopralluoghi** - finalizzati ad accertare la regolarità dell'erogazione dei servizi. Parallelamente, Regione Lombardia effettuerà dei **monitoraggi periodici,** al fine di verificare la corretta e puntuale fruizione dei servizi integrativi richiesti;

- Infine, per poter consentire l'erogazione del rimborso, i soggetti beneficiari saranno tenuti a presentare un'apposita **domanda di liquidazione.** In tale contesto, dopo che le Province e le Città metropolitane avranno dato luogo alla fase **istruttoria delle domande di liquidazione**, i soggetti beneficiari - che ne avranno diritto - saranno rimborsati per le spese sostenute per far fronte all'erogazione dei servizi integrativi in capo ai soggetti disabili coinvolti.

Eventuali note:

_____
_____
_____
_____

2 P2: “FINALITA’ E BASE GIURIDICA”

Categoria di dati trattati e finalità	Specificare su quale base giuridica si basano i trattamenti	Per i casi di “*Compito di interesse pubblico o connesso a esercizio di pubblici poteri del titolare*” e “*Obbligo di legge cui è soggetto il titolare*”, su quale/i norma/e si fonda il trattamento?
Finalità 1: Consentire l’erogazione di una serie di servizi integrativi “al lavoro” e “alla persona” in favore dei soggetti con disabilità **Categoria di dati trattati:** ☒ Dati personali comuni ☒ Categorie particolari di dati personali ☒ Dati relativi a condanne penali o reati	**Il trattamento in oggetto riguarda dati personali comuni ed è giustificato dalle basi giuridiche selezionate:** ☒Compito di interesse pubblico o connesso a esercizio di pubblici poteri del titolare ☐ Obbligo di legge cui è soggetto il titolare ☐ Interesse vitale dell’interessato o di un terzo ☐ Legittimo interesse del titolare o di terzi ☐ Adempimento di obblighi contrattuali ☐ Consenso **Il trattamento in oggetto riguarda “categorie particolari di dati personali” o “dati relativi a condanne penali o reati” ed è giustificato dalle basi giuridiche selezionate:** ☐ l'interessato ha prestato il proprio consenso esplicito ☐il trattamento è 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 ☐ il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; ☐ il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, e il trattamento riguarda unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione. ☐ il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; ☐ il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; ☒ il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, ☐ il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale. ☐ il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica. ☐ il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.	**Normativa di rango primario statale o regionale (legge, decreto-legge, decreto legislativo, etc.)** - Legge 12 marzo 1999 n. 68; - Decreto Legislativo. 10 settembre 2003 n. 276 “*Attuazione delle deleghe in materia di occupazione e mercato del lavoro di cui alla Legge 14 febbraio 2003 n. 30*”; - Decreto Legislativo 14 settembre 2015 n. 150 **Atti di normazione secondaria e delibere di giunta regionale:** - DGR n. X/7763 del 17 gennaio 2018; - DGR n. XII/ 1334 Seduta del 13/11/2023; - DGR 2024 n. XII /3383 del 11 novembre 2024 **La normativa recante disposizioni specifiche in materia di protezione dei dati personali (che può operare anche un rinvio ad altro atto) disciplina i seguenti aspetti del trattamento:** ☒ condizioni relative alla liceità del trattamento ☒ tipologia di dati trattati ☒ interessati ☒ soggetti a cui vengono comunicati i dati ☒ finalità della predetta comunicazione ☒ limitazioni delle finalità ☐ periodi di conservazione ☒ operazioni e procedure di trattamento ☒ misure atte a garantire la liceità e la correttezza del trattamento **Per il caso di trattamento di categorie particolari di dati personali, la normativa recante disposizioni specifiche in materia di protezione dei dati personali disciplina i seguenti aspetti del trattamento:** ☒ tipologia di dati trattati ☒ operazioni di trattamento ☒ motivo di interesse pubblico rilevante

		☐ misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

3 P3: "SOGGETTI COINVOLTI"

3.1 Soggetti che trattano i dati

Indicare la lista delle finalità dei trattamenti (riprese dalla scheda P2 di questo documento)	Indicare il Titolare del trattamento	Indicare gli eventuali responsabili del trattamento (es. fornitori/subfornitori) coinvolti nel trattamento	Indicare gli eventuali Titolari autonomi a cui vengono trasferiti i dati personali
Consentire l'erogazione di una serie di servizi integrativi "al lavoro" e "alla persona" in favore dei soggetti con disabilità	Regione Lombardia	**Responsabili nominati dal Titolare** - ARIA S.p.A. - Province e Città metropolitana (Lombardia)	**Relativamente al trattamento dei dati personali connesso all'esercizio di proprie finalità istituzionali:** • Operatori accreditati al lavoro • Datori di lavoro (eventualmente) • Altri soggetti che partecipano al Comitato Disabili (L.R. 13/03)

3.2 Soggetti interessati di cui vengono trattati i dati

Aspetto	Risposta/Descrizione

Qual è la **tipologia di soggetti interessati coinvolti?**	- Rappresentanti legali; - Soggetti con poteri di firma; - Soggetti con disabilità; - Eventuali tutori legali e/o soggetti che agiscono per conto della persona con disabilità
Fornire una stima del **numero di soggetti interessati coinvolti**	Circa 20.000*

Eventuali note: Trattandosi di una nuova misura, non si può conoscere con esattezza la stima dei soggetti interessati potenzialmente coinvolti*

4 P4: "VALUTAZIONE DI NECESSITA' E PROPORZIONALITA'"

4.1 Dati personali trattati

Indicare le tipologie dei dati da trattare	Fornire il dettaglio dei dati personali da trattare (esempi: nome, codice fiscale, patologia)	Domande utili per comprendere l'effettiva necessità e proporzionalità dei dati rispetto alle finalità	Risposta e giustificazione
Dati personali comuni ☒Dati identificativi diretti ☒Dati identificativi indiretti ☐Stato civile ☐Percorso professionale ☐Dati di connettività ☐Altro **Dati personali comuni percepiti come critici** ☐Dati riguardanti la vita privata ☐Informazioni finanziarie ☐Dati identificativi di conti correnti, carte di debito, credito, etc. ☐Dati sulla posizione ☐Altro	**Dati personali comuni** Soggetti con disabilità: Codice fiscale, nome, cognome, cittadinanza, data e luogo di nascita, indirizzo di residenza/domicilio, e-mail, telefono/cellulare. Rappresentanti legali/soggetti con poteri di firma: Nome, cognome, codice fiscale, data di nascita, cittadinanza. Tutori legali e/o soggetti che agiscono per conto del disabile: Nome, cognome, data e luogo di nascita, codice fiscale, telefono/cellulare, e-mail	**I dati trattati sono limitati, adeguati e pertinenti rispetto alle finalità?** **Per ciascuna categoria/dato giustificare il motivo per il quale il dato è trattato.**	SI I dati personali in questione sono trattati per assicurare il corretto svolgimento dell'intera procedura prevista dalla misura, dalla raccolta delle informazioni necessarie, alla fase di concessione del rimborso in capo ai soggetti beneficiari e anche per poter dar seguito allo svolgimento delle attività istruttorie.

Indicare le tipologie dei dati da trattare	Fornire il dettaglio dei dati personali da trattare (esempi: nome, codice fiscale, patologia)	Domande utili per comprendere l'effettiva necessità e proporzionalità dei dati rispetto alle finalità	Risposta e giustificazione
Categorie particolari di dati personali / Dati personali relativi a condanne penali o reati ☒Dati relativi alla salute ☐Dati relativi alla vita sessuale ☐Dati relativi all'orientamento sessuale ☐Dati biometrici ☐Dati genetici ☒Convinzioni religiose o filosofiche ☒Dati che rivelino l'origine razziale o etnica ☐Dati sull'appartenenza sindacale ☒Dati relativi a condanne penali ☒Dati riguardanti reati ☐Altro	Informazioni correlate alle certificazioni antimafia; stato di disabilità/appartenenza a categorie protette, origine razziale o etnica, convinzioni religiose o filosofiche		
		Nel caso in cui vengano trattate categorie particolari di dati personali, è possibile evitarne il trattamento? motivare la risposta	No, in quanto i destinatari degli interventi previsti dalla misura in questione risultano essere i soggetti con disabilità

Eventuali note:

_____

_____

4.2 Operazioni sui dati

Indicare le operazioni sui dati	Domande utili per comprendere l'effettiva necessità e proporzionalità delle operazioni rispetto alle finalità	Risposta e giustificazione
☒Comunicazione ☒Consultazione ☐Pubblicazione/Diffusione ☒Raccolta ☒Elaborazione ☒Conservazione ☒Interconnessione ☐Altro (specificare) Indicare se i dati vengono raccolti: ☒Direttamente dall'interessato (es. compilazione di un form su una pagina web, compilazione di una scheda di raccolta cartacea, etc.) ☒Indirettamente (es. ottenimento di dati personali da terzi)	**Tutte le operazioni sui dati indicate sono necessarie per il raggiungimento della finalità del trattamento?** **Per ciascuna operazione giustificare per quale motivo viene svolta. Evitare operazioni non necessarie rispetto alle finalità.**	SI **Raccolta**: effettuata per poter disporre di tutte le informazioni necessarie alla gestione delle domande e dei vari iter correlati alla realizzazione della misura (es. controlli, monitoraggio, erogazione del rimborso, etc.); **Consultazione**: necessaria per poter gestire l'intera procedura e richiedere, eventualmente, integrazioni documentali; **Conservazione**: necessaria per poter garantire lo svolgimento dell'intero iter procedurale e per poter dar seguito a successivi controlli da parte di Regione Lombardia; **Interconnessione**: necessaria per poter consentire lo scambio di informazioni tra i vari sistemi regionali, anche al fine di controllare la presenza o meno di alcuni documenti e consentire la prosecuzione dell'iter finalizzato all'ottenimento del rimborso; **Comunicazione**: necessaria nei confronti di Province e Città metropolitane, al fine di fornire loro tutte le informazioni utili ad esperire le varie fasi procedurali previste per l'erogazione dei servizi al lavoro e alla persona; **Elaborazione**: necessaria per evitare l'identificazione dei soggetti interessati in occasione di pubblicazioni e attività di monitoraggio (anonimizzazione).

Indicare le operazioni sui dati	Domande utili per comprendere l'effettiva necessità e proporzionalità delle operazioni rispetto alle finalità	Risposta e giustificazione
	Vi è una pubblicazione o diffusione di dati personali? A quale scopo? Risulta applicabile/da applicare il principio di trasparenza?	NO
	È necessario realizzare copie dei dati personali (esempio: copie dell'archivio)? motivare la risposta	NO
	Le operazioni indicate includono l'impiego di algoritmi decisionali/trattamenti automatizzati che producono effetti giuridici sugli interessati?	NO
	Viene effettuata profilazione?	NO

4.3 Accesso ai dati personali

Indicare i soggetti preposti al trattamento dei dati e i relativi privilegi di accesso	Risposta e giustificazione	Domande utili per comprendere l'effettiva necessità e proporzionalità dell'accesso ai dati	Risposta e giustificazione
Quali sono i soggetti preposti al trattamento che accedono ai dati personali?	**Soggetti interni autorizzati** ☒Soggetti appartenenti agli Enti ☒Soggetti della funzione sistemi informativi ☒Soggetti delle funzioni di audit e compliance **Soggetti esterni autorizzati** ☒ Funzioni di help desk ☒ Funzioni di supporto sistemistico ☒Dipendenti di enti pubblici es. Comuni, Ministeri etc. (Comuni e Province) ☒Altri soggetti di altre società esterne - ARIA S.p.A.; - Personale di assistenza tecnica agli Uffici di Regione Lombardia; - Operatori delle Province e delle Città metropolitane	**Per ciascuna tipologia di utenti che accede ai dati personali indicare il motivo per il quale è concesso l'accesso.**	- **Regione Lombardia,** in qualità di titolare del trattamento - **ARIA S.p.A.** (responsabile nominato dal titolare) Preposta all'assistenza funzionale e sistemistica delle piattaforme e dei sistemi utilizzati da Regione Lombardia. - **Gli operatori delle Province e delle Città metropolitane** (responsabili del trattamento) che ricevono e gestiscono le domande presentate dai soggetti destinatari della misura e che svolgono un ruolo importante durante la gestione dell'intero processo finalizzato all'erogazione dei servizi in capo ai soggetti disabili.

Indicare i soggetti preposti al trattamento dei dati e i relativi privilegi di accesso	Risposta e giustificazione	Domande utili per comprendere l'effettiva necessità e proporzionalità dell'accesso ai dati	Risposta e giustificazione
		L'accesso è necessario/limitato rispetto alle attività che devono essere svolte?	SI
		Per ciascuna tipologia di utenti sono stati stabiliti i privilegi di accesso?	SI
		I privilegi di accesso sono necessari/limitati rispetto alle attività che devono essere svolte?	SI

Eventuali note:

_____
_____
_____
_____

5 P5: “DATA RETENTION”

Tipologia dei dati trattati	Quantificare il tempo di conservazione dei dati.	C’è una legge che lo giustifica? Se si indicare quale Altrimenti fornire il criterio utilizzato per determinarlo
Dati dell’iniziativa/misura/servizio che stai considerando	I dati personali raccolti saranno conservati per un periodo di tempo pari a 10 anni dalla conclusione delle azioni previste all'interno del protocollo di riferimento della misura.	Art. 2220 c.c.

Eventuali note:

_____
_____
_____
_____

6 P6: "DPIA: QUANDO E PERCHE'"

L'iniziativa/misura/servizio ricade in uno di questi casi?	Si/No
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*".	NO
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).	NO
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.	NO
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).	NO
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).	NO

Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).	**SI**
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.	NO
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.	NO
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*).	NO
Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.	**SI**
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	NO
Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	NO

Eventuali note:

7 P8: "IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA"

Piattaforma BeS

Valutazione dei rischi	Risultanze
È prevista l'esecuzione dell'Analisi dei Rischi da parte del fornitore servizio IT (es: Aria)?	☒Sì ☐No
È stata già svolta un'analisi dei Rischi sul servizio da parte del fornitore (es: Aria)?	☒Sì ☐No

Al fine di verificare il livello di implementazione delle misure di sicurezza e conseguentemente le modalità mediante le quali il rischio intrinseco risulta essere mitigato, si riportano di seguito le contromisure, raggruppate in diverse aree.
Per ogni singola misura indicare il livello di implementazione ("Si" la misura è applicabile/applicata; "In parte" la misura è parzialmente applicabile/applicata; "No" la misura non risulta applicata; "N/A" la misura non è applicabile).

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Change Management	**È previsto che le attività di Change Management, svolte sul sistema, vengano gestite in accordo con le politiche e le procedure definite dall'organizzazione?**	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che le attività di sviluppo e di test delle modifiche, effettuate sul sistema, vengano eseguite in ambienti dedicati, separati	☒ Si ☐ In parte ☐ No ☐ N/A	……

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	dall'ambiente di produzione?		
Access Management	**È previsto che le utenze abilitate ad accedere al sistema vengano create, modificate, riviste e cancellate,**	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che l'accesso al sistema avvenga attraverso una combinazione di username e password?	☐ Si ☐ In parte ☐ No ☒ N/A	L'autenticazione a Sistema è possibile attraverso SPID, IDPC e CIE.
	È prevista e implementata una password policy che definisca la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili?	☐ Si ☐ In parte ☐ No ☒ N/A	L'autenticazione a Sistema è possibile attraverso SPID, IDPC e CIE.
	È previsto che i diritti di accesso al sistema, assegnati agli utenti, vengano rilasciati in base al principio della stretta pertinenza, del minimo privilegio e necessità per il ruolo di accedere e conoscere i dati (principio del need to know)?	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che per l'accesso ai sistemi venga richiesto un sistema di multi factor authentication?	☒ Si ☐ In parte ☐ No ☐ N/A	L'autenticazione a Sistema è possibile attraverso SPID, IDPC e CIE.

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Logging&Monitoring	**È prevista la generazione di file di log per tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione) con il dettaglio della data e dell'ora?**	☒ Si ☐ In parte ☐ No ☐ N/A	Centralizzato su IDPC
	È previsto che i file di log siano adeguatamente protetti da manomissioni e accessi non autorizzati?	☒ Si ☐ In parte ☐ No ☐ N/A	Centralizzato su IDPC
	È previsto che le attività degli amministratori di sistema vengano registrate, analizzate e riviste periodicamente?	☐ Si ☒ In parte ☐ No ☐ N/A	……
Server/Database security	**È previsto che vengano applicate tecniche di cifratura e pseudonimizzazione sui server/database, in funzione della tipologia di dati trattati?**	☐ Si ☐ In parte ☐ No ☒ N/A	
Cifratura delle comunicazioni	**È previsto che i dati personali in fase di trasmissione siano cifrati o vengano utilizzati canali sicuri per la trasmissione (e.g. SSH, HTTPS) o per le comunicazioni (e.g. firewall, IPS/IDS)?**	☒ Si ☐ In parte ☐ No ☐ N/A	https
Sicurezza delle applicazioni	**È prevista, per il servizio, l'esecuzione di attività di Vulnerability assessment e Penetration test?**	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che le patch e gli aggiornamenti di sicurezza, relativi al servizio, siano testati e approvati prima di	☒ Si ☐ In parte ☐ No	……

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	essere installati sull'ambiente di produzione?	☐ N/A	
Back-up Management	**È previsto che i dati siano sottoposti a backup periodici, in accordo con il piano di schedulazione definito in un'apposita procedura?**	☒ Si ☐ In parte ☐ No ☐ N/A	.....
	È previsto che l'esecuzione del backup del sistema venga monitorato?	☒ Si ☐ In parte ☐ No ☐ N/A	.....
	È previsto vengano effettuati test periodici di Restore del Backup e test del Disaster Recovery?	☒ Si ☐ In parte ☐ No ☐ N/A	.....
Gestione degli incidenti di sicurezza	**È previsto che in caso di incidente vi sia una risposta rapida ed efficace, in accordo con la procedura definita dall'organizzazione?**	☒ Si ☐ In parte ☐ No ☐ N/A	.....
	È previsto che in caso di Data Breach venga seguita la procedura di Data Breach definita dall'organizzazione?	☒ Si ☐ In parte ☐ No ☐ N/A	.....
Formazione in materia di sicurezza dell'informazione	**È previsto che i dipendenti ricevano adeguata formazione/attività di sensibilizzazione in materia di protezione dei dati?**	☒ Si ☐ In parte ☐ No ☐ N/A	.....
Sicurezza fisica	**È prevista l'applicazione di adeguate misure di sicurezza fisica presso le aree critiche (e.g. sale CED)?**	☒ Si ☐ In parte ☐ No ☐ N/A	.....

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Gestione del Rischio	**È prevista l'esecuzione dell'analisi dei Rischi IT per il servizio da parte del fornitore?**	☒ Si ☐ In parte ☐ No ☐ N/A	……
Gestione delle Terze Parti	**È prevista la definizione di istruzioni e l'accordo di nomina a Responsabile per le Terze parti coinvolte?**	☒ Si ☐ In parte ☐ No ☐ N/A	……
Sicurezza dei documenti cartacei	**È previsto, nel caso il trattamento preveda l'utilizzo di dati cartacei, che quest'ultimi vengano gestiti in accordo con la politica definita dall'organizzazione?**	☐ Si ☐ In parte ☒ No ☐ N/A	……

SIUL

Valutazione dei rischi	Risultanze
È prevista l'esecuzione dell'Analisi dei Rischi?	☒Sì ☐No
È stata svolta un'analisi dei Rischi sul servizio?	☒Sì ☐No
Se sì, procedere con la compilazione della seguente sezione utilizzando il tool di Analisi dei Rischi semplificata o approfondita. **Nel caso in cui non fosse stata effettuata o non fosse stata prevista un'Analisi dei Rischi, procedere alla compilazione richiedendo il supporto al Service Manager e/o al fornitore del servizio.**	

Al fine di verificare il livello di implementazione delle misure di sicurezza e conseguentemente le modalità mediante le quali il rischio intrinseco risulta essere mitigato, si riportano di seguito le contromisure, raggruppate in diverse aree.

Per ogni singola misura indicare il livello di implementazione (“Si” la misura è applicabile; “In parte” la misura è parzialmente applicata; “No” la misura non risulta applicata; “N/A” la misura non è applicabile) e, ove presente, il riferimento al controllo analizzato mediante l’attività di Analisi dei Rischi (AdR).

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Change Management	**È previsto che le attività di Change Management, svolte sul sistema, vengano gestite in accordo con le politiche e le procedure definite dall'organizzazione?**	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto che le attività di sviluppo e di test delle modifiche, effettuate sul sistema, vengano eseguite in ambienti dedicati, separati dall'ambiente di produzione?	☒ Si ☐ In parte ☐ No ☐ N/A	
Access Management	**È previsto che le utenze abilitate ad accedere al sistema vengano create, modificate, riviste e cancellate, in accordo con la procedura di gestione degli accessi logici definita dall'organizzazione?**	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto che l’accesso al sistema avvenga attraverso una combinazione di username e password?	☐ Si ☐ In parte ☐ No ☒ N/A	L’autenticazione a sistema è possibile attraverso tre modalità: SPID, EIDAS, IDPC e CIE.
	È prevista e implementata una password policy che definisca la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili?	☐ Si ☐ In parte ☐ No ☒ N/A	L’autenticazione a sistema è possibile attraverso tre modalità: SPID, EIDAS, IDPC e CIE.

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	È previsto che i diritti di accesso al sistema, assegnati agli utenti, vengano rilasciati in base al principio della stretta pertinenza, del minimo privilegio e necessità per il ruolo di accedere e conoscere i dati (principio del need to know)?	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto che per l'accesso ai sistemi venga richiesto un sistema di multi factor authentication?	☒ Si ☐ In parte ☐ No ☐ N/A	L'autenticazione a sistema è possibile attraverso tre modalità: SPID, EIDAS, IDPC e CIE.
Logging&Monitoring	**È prevista la generazione di file di log per tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione) con il dettaglio della data e dell'ora?**	☒ Si ☐ In parte ☐ No ☐ N/A	Delegato a IDPC
	È previsto che i file di log siano adeguatamente protetti da manomissioni e accessi non autorizzati?	☒ Si ☐ In parte ☐ No ☐ N/A	Delegato a IDPC
	È previsto che le attività degli amministratori di sistema vengano registrate, analizzate e riviste periodicamente?	☒ Si ☐ In parte ☐ No ☐ N/A	
Server/Database security	**È previsto che vengano applicate tecniche di cifratura e pseudonimizzazione sui server/database, in funzione della tipologia di dati trattati?**	☒ Si ☐ In parte ☒ No ☐ N/A	Cifratura del DB in TDE – Transparent Data Encryption

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Cifratura delle comunicazioni	**È previsto che i dati personali in fase di trasmissione siano cifrati o vengano utilizzati canali sicuri per la trasmissione (e.g. SSH, HTTPS) o per le comunicazioni (e.g. firewall, IPS/IDS)?**	☒ Si ☐ In parte ☐ No ☐ N/A	HTTPS
	È previsto, all'interno del contratto con i fornitori/subfornitori che hanno accesso al servizio, che venga abilitata la crittografia del disco sulle unità del sistema operativo della workstation della postazione di lavoro?	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto che l'accesso avvenga tramite VPN? **È previsto/sarà previsto anche all'interno del contratto con i fornitori/subfornitori?**	☒ Si ☐ In parte ☐ No ☐ N/A ☒Sì ☐No	
Utilizzo dei dispositivi portatili	**È previsto che vengano applicate le politiche di gestione sicura dei dispositivi mobili e portatili?** **È previsto/sarà previsto anche all'interno del contratto con i fornitori/subfornitori?**	☒ Si ☐ In parte ☐ No ☐ N/A ☒Sì ☐No	

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	È previsto che vengano utilizzati strumenti o software per la protezione ed il controllo dei dispositivi mobili e portabili (e.g. MDM/MAM)?	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto/sarà previsto, all'interno del contratto con i fornitori/subfornitori?	☒Sì ☐No	
	È prevista, per il servizio, l'esecuzione di attività di Vulnerability assessment e Penetration test?	☒ Si ☐ In parte ☐ No ☐ N/A	
Sicurezza delle applicazioni	**È previsto che le patch e gli aggiornamenti di sicurezza, relativi al servizio, siano testati e approvati prima di essere installati sull'ambiente di produzione?**	☒ Si ☐ In parte ☐ No ☐ N/A	
Back-up Management	**È previsto che i dati siano sottoposti a backup periodici, in accordo con il piano di schedulazione definito in un'apposita procedura?**	☒ Si ☐ In parte ☐ No ☐ N/A	

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	È previsto che l'esecuzione del backup del sistema venga monitorato, in accordo con quanto definito dalla procedura definita dall'organizzazione?	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto vengano effettuati test periodici di Restore del Backup e test del Disaster Recovery?	☒ Si ☐ In parte ☐ No ☐ N/A	
Gestione degli incidenti di sicurezza	**È previsto che in caso di incidente vi sia una risposta rapida ed efficace, in accordo con la procedura definita dall'organizzazione?**	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto che in caso di Data Breach venga seguita la procedura di Data Breach definita dall'organizzazione?	☒ Si ☐ In parte ☐ No ☐ N/A	
Formazione in materia di sicurezza dell'informazione	**È previsto che i dipendenti ricevano adeguata formazione/attività di sensibilizzazione in materia di protezione dei dati?**	☒ Si ☐ In parte ☐ No ☐ N/A	
Sicurezza fisica	**È prevista l'applicazione di adeguate misure di sicurezza fisica presso le aree critiche (e.g. sale CED)?**	☒ Si ☐ In parte ☐ No ☐ N/A	
Gestione del Rischio	**È prevista l'esecuzione dell'analisi dei Rischi IT per il servizio?**	☒ Si ☐ In parte ☐ No ☐ N/A	

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Sicurezza dei documenti cartacei	**È previsto, nel caso il trattamento preveda l'utilizzo di dati cartacei, che quest'ultimi vengano gestiti in accordo con la politica definita dall'organizzazione?**	☐ Si ☐ In parte ☐ No ☒ N/A	

Piattaforma SIUO

Valutazione dei rischi	Risultanze
È prevista l'esecuzione dell'Analisi dei Rischi da parte del fornitore servizio IT?	☒Sì ☐No
È stata già svolta un'analisi dei Rischi sul servizio da parte del fornitore?	☐Sì ☒No

Al fine di verificare il livello di implementazione delle misure di sicurezza e conseguentemente le modalità mediante le quali il rischio intrinseco risulta essere mitigato, si riportano di seguito le contromisure, raggruppate in diverse aree.

Per ogni singola misura indicare il livello di implementazione ("Si" la misura è applicabile/applicata; "In parte" la misura è parzialmente applicabile/applicata; "No" la misura non risulta applicata; "N/A" la misura non è applicabile).

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	È previsto che le attività di Change Management, svolte sul sistema, vengano gestite in accordo con le politiche	☒ Si ☐ In parte ☐ No ☐ N/A	……

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Change Management	**e le procedure definite dall'organizzazione?**		
	È previsto che le attività di sviluppo e di test delle modifiche, effettuate sul sistema, vengano eseguite in ambienti dedicati, separati dall'ambiente di produzione?	☒ Si ☐ In parte ☐ No ☐ N/A	
Access Management	**È previsto che le utenze abilitate ad accedere al sistema vengano create, modificate, riviste e cancellate, in accordo con la procedura di gestione degli accessi logici definita dall'organizzazione?**	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che l'accesso al sistema avvenga attraverso una combinazione di username e password?	☐ Si ☐ In parte ☐ No ☒ N/A	L'autenticazione a sistema è possibile attraverso le modalità: SPID, TS-CNS, CIE.
	È prevista e implementata una password policy che definisca la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili?	☐ Si ☐ In parte ☐ No ☒ N/A	L'autenticazione a sistema è possibile attraverso le modalità: SPID, TS-CNS, CIE.

Il presente documento, in formato cartaceo, è da considerarsi FUORI CONTROLLO salvo presenza della firma di chi approva ed emette il documento stesso

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	È previsto che i diritti di accesso al sistema, assegnati agli utenti, vengano rilasciati in base al principio della stretta pertinenza, del minimo privilegio e necessità per il ruolo di accedere e conoscere i dati (principio del need to know)?	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che per l'accesso ai sistemi venga richiesto un sistema di multi factor authentication?	☒ Si ☐ In parte ☐ No ☐ N/A	L'autenticazione a sistema è possibile attraverso le modalità: SPID, TS-CNS, CIE.
Logging&Monitoring	**È prevista la generazione di file di log per tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione) con il dettaglio della data e dell'ora?**	☐ Si ☒ In parte ☐ No ☐ N/A	
	È previsto che i file di log siano adeguatamente protetti da manomissioni e accessi non autorizzati?	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto che le attività degli amministratori di sistema vengano registrate, analizzate e riviste periodicamente?	☒ Si ☐ In parte ☐ No ☐ N/A	……
Server/Database security	**È previsto che vengano applicate tecniche di cifratura e pseudonimizzazione sui server/database, in funzione della tipologia di dati trattati?**	☐ Si ☐ In parte ☒ No ☐ N/A	

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Cifratura delle comunicazioni	**È previsto che i dati personali in fase di trasmissione siano cifrati o vengano utilizzati canali sicuri per la trasmissione (e.g. SSH, HTTPS) o per le comunicazioni (e.g. firewall, IPS/IDS)?**	☒ Si ☐ In parte ☐ No ☐ N/A	
Sicurezza delle applicazioni	**È prevista, per il servizio, l'esecuzione di attività di Vulnerability assessment e Penetration test?**	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto che le patch e gli aggiornamenti di sicurezza, relativi al servizio, siano testati e approvati prima di essere installati sull'ambiente di produzione?	☒ Si ☐ In parte ☐ No ☐ N/A	
Back-up Management	**È previsto che i dati siano sottoposti a backup periodici, in accordo con il piano di schedulazione definito in un'apposita procedura?**	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che l'esecuzione del backup del sistema venga monitorato?	☒ Si ☐ In parte ☐ No ☐ N/A	
	È previsto vengano effettuati test periodici di Restore del Backup e test del Disaster Recovery?	☒ Si ☐ In parte ☐ No ☐ N/A	

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
Gestione degli incidenti di sicurezza	**È previsto che in caso di incidente vi sia una risposta rapida ed efficace, in accordo con la procedura definita dall'organizzazione?**	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che in caso di Data Breach venga seguita la procedura di Data Breach definita dall'organizzazione?	☒ Si ☐ In parte ☐ No ☐ N/A	……
Formazione in materia di sicurezza dell'informazione	**È previsto che i dipendenti ricevano adeguata formazione/attività di sensibilizzazione in materia di protezione dei dati?**	☒ Si ☐ In parte ☐ No ☐ N/A	……
Sicurezza fisica	**È prevista l'applicazione di adeguate misure di sicurezza fisica presso le aree critiche (e.g. sale CED)?**	☒ Si ☐ In parte ☐ No ☐ N/A	
Gestione del Rischio	**È prevista l'esecuzione dell'analisi dei Rischi IT per il servizio da parte del fornitore?**	☒ Si ☐ In parte ☐ No ☐ N/A	
Gestione delle Terze Parti	**È prevista la definizione di istruzioni e l'accordo di nomina a Responsabile per le Terze parti coinvolte?**	☒ Si ☐ In parte ☐ No ☐ N/A	
Sicurezza dei documenti cartacei	**È previsto, nel caso il trattamento preveda l'utilizzo di dati cartacei, che quest'ultimi vengano gestiti in accordo con la politica definita dall'organizzazione?**	☒ Si ☐ In parte ☐ No ☐ N/A	

8 P8: “ADEMPIMENTI PRIVACY”

Adempimenti per la protezione dei dati personali (selezionare le operazioni da svolgere)

☒ Segnalare al proprio referente privacy di aggiornare il registro dei trattamenti.
☒ Redazione/aggiornamento di contratti/nomine verso tutte le parti coinvolte.
☒ Redazione dell’informativa privacy e caricamento sulla piattaforma.
L’informativa verrà fornita ai soggetti interessati secondo le modalità di seguito riportate:

Informativa privacy allegata all’avviso

☒ Definire le modalità tecniche per la cancellazione dei dati personali secondo i periodi di data retention individuati.
☒ Utilizzare gli strumenti per gestire le richieste degli interessati (reclami, richieste di rettifica e/o cancellazione dei dati personali)
☒ Archiviare presso la DG competente il presente verbale e trasmetterlo formalmente al Privacy Officer

Eventuali note:
_____
_____
_____
_____

Allegato 1: "ANALISI INTEGRATIVA PER TRATTAMENTI DA SOTTOPORRE A DPIA"

La parte di documento che segue è da compilare soltanto qualora nella scheda P6 "DPIA: QUANDO E PERCHE'" della Privacy by Design, si abbia risposto "Sì" ad una o più domande o qualora il trattamento presenti rischi elevati per i diritti e le libertà degli interessati.

1. Valutazioni giuridiche

1.1 Valutazioni sul rispetto del principio di trasparenza

Analisi della trasparenza del trattamento	Risultanze
I dati personali vengono raccolti presso l'interessato o provengono da terze parti?	I dati personali dei soggetti interessati sono raccolti direttamente (per il tramite delle piattaforme regionali) e indirettamente (per quanto attiene alle informazioni eventualmente raccolte dai soggetti beneficiari, esecutori della misura)
Verrà/è stata predisposta un'informativa sul trattamento dei dati personali?	☒Sì ☐No
Se no, motivare	☐Non è stata ancora predisposta l'informativa ☐Ricorre un'eccezione all'obbligo di fornire l'informativa all'interessato
Se sì, l'informativa è stata formulata con un linguaggio chiaro e semplice per l'interessato?	Sì, è stata formulata secondo il template in uso presso Regione Lombardia
Tale documento contiene gli elementi essenziali richiesti dal GDPR?	☒Indicazione del Titolare del trattamento e relativi dati di contatto ☒Dati di contatto del Responsabile della Protezione dei Dati ("RPD" o "DPO") ☒Finalità del trattamento ☒Base giuridica ☒Destinatari e categorie di destinatari dei dati personali: ☒ Titolari autonomi ☒ Responsabili del trattamento ☒Periodo di conservazione dei dati personali ☒Diritti degli interessati e dati di contatto per il loro esercizio

	☒Diritto di proporre reclamo all'Autorità Garante
Qualora vi fosse un trasferimento di dati personali al di fuori dello Spazio Economico Europeo, questo è stato indicato nell'informativa?	N/A
Qualora il trattamento si fondasse sul consenso dell'interessato, è stata indicata la possibilità di revocare il consenso prestato?	N/A
Qualora vi sarà/fosse un processo decisionale automatizzato o sarà/venisse effettuata un'attività di profilazione, saranno/sono state rese informazioni sulle logiche di profilazione e sulle conseguenze del trattamento?	N/A
Informazioni aggiuntive/eventuali note: ……	

1.2 Valutazioni sul rispetto del principio di accuratezza

Analisi dell'accuratezza dei dati personali	Risultanze	
Il sistema informatico verrà/è stato configurato in modo da permettere la cancellazione dei dati personali inesatti?	☒Sì	☐No
Il sistema informatico verrà/è stato configurato in modo da permettere la modifica dei dati personali inesatti?	☒Sì	☐No
Il sistema informatico verrà/è stato configurato in modo da permettere l'aggiornamento dei dati personali inesatti?	☒Sì	☐No
Se una delle precedenti risposte è sì, sarà/è stato definito un processo e/o saranno/sono stati individuati i soggetti preposti per la cancellazione, modifica, aggiornamento dei dati?	**SI**	
Informazioni aggiuntive/eventuali note: ……		

1.3 Valutazioni sul rispetto dei diritti e delle libertà fondamentali della persona

Rispetto dei diritti e libertà fondamentali della persona	Risultanze
Il trattamento potrebbe comportare la lesione di un diritto o libertà fondamentale dell'interessato (ad esempio: Libertà di pensiero, Libertà di espressione, Diritto alla salute, etc.)**?**	☒Sì ☐No
Se sì, specificare quale	Il trattamento dei dati personali potrebbe comportare la lesione del diritto alla riservatezza
In un'ottica di bilanciamento di interessi, qualora il trattamento comporti la compressione di un diritto fondamentale o una libertà, tale compressione è giustificata da un beneficio reso all'interessato?	☒Sì ☐No
Se sì, specificare il beneficio reso all'interessato con il trattamento	Senza il trattamento dei dati personali in questione, in tale contesto, non sarebbe possibile, per i soggetti interessati coinvolti, beneficiare dei servizi integrativi "al lavoro" e "alla persona".
Il trattamento assicura la parità tra i soggetti interessati evitando discriminazioni irragionevoli (limitazioni ingiustificate all'accesso ai servizi della P.A., disparità di trattamento immotivate, preclusioni all'accesso a servizi, etc.)**?**	☒Sì ☐No
Il trattamento si traduce in una delle seguenti operazioni?	☐Valutazione degli interessati su larga scala con attribuzione di punteggio (scoring), profilazione, divisione in classi ☐Processi decisionali automatizzati ☐Controllo e monitoraggio sistematico dell'interessato ☐Utilizzo di tecnologie innovative (sistemi di riconoscimento facciale, blockchain, intelligenza artificiale, machine learning, etc.) ☒N/A

Sono state implementate misure specifiche per la riduzione dei rischi connessi, di cui al punto precedente?	☐Sì ☒No
Se sì, quali? (consultare il manuale per esempi di contromisure)	……

Informazioni aggiuntive/eventuali note: ……

1.4 Diritti esercitabili dall'interessato

Diritti dell'interessato	Possibilità di esercizio del diritto	
Diritto di accesso dell'interessato	☒Sì	☐No
Diritto di rettifica	☒Sì	☐No
Diritto alla cancellazione	☐Sì	☒No
Diritto di limitazione del trattamento	☒Sì	☐No
Diritto alla portabilità dei dati	☐Sì	☒No
Diritto di opposizione	☒Sì	☐No

Rimane impregiudicato - nel caso in cui sia necessario il consenso esplicito - il diritto dell'interessato all'esercizio alle informazioni e all'accesso ai dati personali, nonché alla loro rettifica e cancellazione.

Quali canali di comunicazione verranno/sono destinati a permettere agli interessati di esercitare i propri diritti? Sarà/è stata individuata una casella mail dedicata?

Sì

E-mail: lavoro@pec.regione.lombardia.it

Informazioni aggiuntive/eventuali note: nella documentazione di riferimento vengono riportati anche i dati della Direzione

D.G. Istruzione, Formazione, Lavoro
U.O. SISTEMA E SERVIZI TERRITORIALI PER IL LAVORO
Piazza Città di Lombardia, 1 – 20124 Milano

1.5 Valutazione dei rischi per i diritti e le libertà degli interessati – rischio informatico

L'impatto privacy è valutato considerando la descrizione presente nella seguente tabella di valutazione dell'impatto.

Valore Qualitativo	Descrizione
Impatto basso	Gli individui possono andare incontro a conseguenze minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Impatto medio	Gli individui possono andare incontro a significative conseguenze, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Impatto alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Impatto molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Area di valutazione	Bene giuridico leso	Impatto	Motivazione del livello di impatto indicato	Quali misure specifiche saranno/sono state previste per l'attenuazione del rischio?
Qualora i dati personali trattati venissero pubblicati o diffusi, quali ipotetici pregiudizi potrebbero prodursi ai danni dell'interessato?	☒Lesione del diritto alla riservatezza ☐Danno di natura fisica ☒Danno di natura psicologica ☐Danno di tipo economico-patrimoniale	☐Basso ☒Medio ☐Alto ☐Molto alto	Nel caso in cui i dati personali trattati venissero illecitamente pubblicati o diffusi, i soggetti interessati coinvolti potrebbero subire eventuali danni di natura psicologica, correlati al timore – soprattutto per quanto attiene ai dati personali relativi a condanne penali	☐Pseudonimizzazione ☐Anonimizzazione ☒Cifratura ☒Procedure di log-on sicure ☐ Altro: ……

	☐Danno connesso alla perdita di chance		e/o reati e alle categorie particolari di dati personali – di essere giudicati e/o eventualmente esclusi da determinati contesti sociali.	
Qualora i dati personali venissero modificati o alterati, quali ipotetici pregiudizi potrebbero prodursi ai danni dell'interessato?	☒Lesione del diritto alla riservatezza ☐Danno di natura fisica ☐Danno di natura psicologica ☐Danno di tipo economico-patrimoniale ☒Danno connesso alla perdita di chance	☐Basso ☒Medio ☐Alto ☐Molto alto	Nel caso in cui i dati personali trattati fossero soggetti ad eventuali modifiche e/o alterazioni non autorizzate, gli interessati potrebbero avere difficoltà nel gestire le procedure correlate alla presentazione della domanda (rappresentanti legali o soggetti con poteri di firma) e/o a poter beneficiare dei servizi integrativi previsti dalla misura (soggetti con disabilità). Una tale circostanza potrebbe pregiudicare negativamente anche le attività di ispezione e di monitoraggio.	☒ Registrazione e de-registrazione degli accessi degli utenti ☐ Riesame dei diritti di accesso degli utenti ☒ Monitoraggio dei Log delle attività ☐Altro: ……
Qualora i dati personali non fossero più disponibili, quali ipotetici pregiudizi potrebbero prodursi ai danni dell'interessato?	☐Lesione del diritto alla riservatezza ☐Danno di natura fisica ☐Danno di natura psicologica ☐Danno di tipo economico-patrimoniale ☒Danno connesso alla perdita di chance	☐Basso ☒Medio ☐Alto ☐Molto alto	L'eventuale indisponibilità temporanea dei dati personali trattati potrebbe comportare l'impossibilità per il soggetto interessato e, dunque, per i soggetti beneficiari coinvolti di ottenere il rimborso e di poter beneficiare dei servizi integrativi previsti dalla misura.	☒Copie di backup ☒Sistemi in Disaster Recovery ☐ Procedure di Business Continuity ☐Altro: ……

Informazioni aggiuntive/eventuali note: ……

1.6 Valutazione giuridica finale sul trattamento

Valutazione giuridica sintetica	Risultanze	Note di commento e approfondimento

Rispetto del principio di liceità: il trattamento si fonda su idonea base giuridica e persegue finalità determinate ed individuate? Cfr. Par. 2 della Privacy by Design	☒Sì	☐No	☐In parte	……..
Rispetto del principio di trasparenza: è stata resa idonea informativa al trattamento dei dati personali agli interessati? Cfr. Par. 1.1 dell'Allegato 1	☒Sì	☐No	☐In parte	……
Rispetto del principio di necessità e proporzionalità: i dati personali trattati, le operazioni effettuate e gli accessi degli operatori ai dati sono solo quelli strettamente necessari al perseguimento delle finalità? Cfr. Par. 4 della Privacy by Design	☒Sì	☐No	☐In parte	…… ……
Rispetto dei diritti fondamentali dell'interessato: il trattamento comporta una compressione dei diritti e delle libertà degli interessati accettabile e giustificabile rispetto alle utilità conseguite dall'interessato? Cfr. Par. 1.3 dell'Allegato 1	☒Sì	☐No	☐In parte	

Informazioni aggiuntive/eventuali note: ……

2. Valutazioni in materia di sicurezza

2.1 Valutazione dei Rischi (SIUL, SIUO, BeS)

La valutazione dei rischi si suddivide sulla base della violazione di riservatezza, integrità e disponibilità delle informazioni trattate, come riportato nella seguente tabella (Cfr. P7 della Privacy by Design):

Tipologia di rischio	*Esempi di eventi correlati al rischio*	*Guida alla determinazione del livello di rischio*	*Valutazione del rischio effettivo (valore qualitativo)*	*Note di commento e approfondimento*
Rischio di perdita di riservatezza dei dati	*Accesso alle informazioni da parte di persone non autorizzate, divulgazione non autorizzata delle informazioni.*	*È presente una segregazione dei ruoli relativamente gli utenti che accedono al sistema? Sono presenti procedure di log-on sicure?*	☒Basso ☐Medio ☐Alto ☐Molto alto	……
Rischio di perdita di integrità dei dati	*Alterazione delle informazioni, recupero di documenti scartati.*	*Vi è il tracciamento dei log relativamente agli accessi? I dati sono conservati in modo sicuro?*	☒Basso ☐Medio ☐Alto ☐Molto alto	……
Rischio di perdita di disponibilità dei dati	*Indisponibilità delle linee di comunicazione e dei sistemi hardware.* *Perdita di disponibilità dei dati trattati a seguito di un incendio, allagamento, etc.*	*Sono previsti sistemi di backup? Sono previsti protocolli di sicurezza utili a garantire l'erogazione del servizio anche in caso di interruzione?* *Sono previste misure di sicurezza come antiincendio, antiallagamento, etc.?*	☒Basso ☐Medio ☐Alto ☐Molto alto	……

3. Considerazioni del Titolare del Trattamento

Il sottoscritto Paolo Mora in qualità di Direttore Generale della Direzione Istruzione, Formazione, Lavoro responsabile dell'attività di analisi, dichiara:

✓ Di aver effettuato e formalizzato le valutazioni di legittimità, necessità e proporzionalità richieste dalla normativa nonché la valutazione e la gestione dei rischi legati al trattamento in oggetto.

✓ Di aver aggiornato il registro dei trattamenti.

La DPIA o valutazione di impatto è prevista dall'art. 35 del Regolamento Europeo e consiste nell'applicazione di un processo volto a descrivere i trattamenti, valutarne la necessità e aiutare a gestire i rischi per i diritti delle persone fisiche derivanti dal trattamento, valutandoli e determinando le misure per indirizzarli.

Sono stati compilati i documenti:

- VERBALE - PRIVACY BY DESIGN E DPIA
- ALLEGATO 1 - ANALISI INTEGRATIVA PER TRATTAMENTI DA SOTTOPORRE A DPIA.

così come previsto della normativa, per ogni piattaforma impattante.

La valutazione del rischio rientra tra i parametri di sicurezza secondo quanto disposto dal Regolamento UE 2016/679.

Privacy Officer:

Dr. Gianluca Jesu

PAOLO MORA
23.10.2025
08:29:07
GMT+01:00

Per la Direzione Istruzione, Formazione, Lavoro il Titolare del trattamento: Paolo Mora

Dirigente competente per il procedimento: Monica Mussetti

EQ competente per il trattamento: Andrea Cremonesi

Dirigente referente privacy: Brunella Reverberi

EQ supporto referente privacy: Andrea Lazzarotti

Per la U.O. Trasformazione digitale per la modernizzazione e la semplificazione: Silvia Eugenia Ronzio

Per ARIA S.p.A.: Stefano Ruta

Firmato da:
CRMNDR75D01F205Z
Codice fiscale: CRMNDR75D01F205Z
Organizzazione: Actalis S.p.A.
Valido da: 22-10-2025 14:36:45 a: 20-10-2031 23:00:00
Certificato emesso da: Regione Lombardia - CA Cittadini 2020, Actalis S.p.A., IT
Riferimento temporale 'SigningTime': 24-11-2025 14:17:05
Motivo: Approvo il documento

Firmato da:
BRUNELLA MARIA GRAZIA REVERBERI
Codice fiscale: RVRBNL58S55F205N
Valido da: 15-03-2024 11:48:25 a: 15-03-2027
Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT
Riferimento temporale 'SigningTime': 20-10-2025 12:40:42
Motivo: Approvo il documento

SILVIA EUGENIA RONZIO
19.11.2025 17:05:59
GMT+01:00