Verbale

# “Privacy By design”

**BANDO**

**“VINNOVATE OPEN CALL 2025 LOMBARDIA**

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

| Revisione | Data | Sintesi delle Modifiche |
|---|---|---|
| *1* | *31.07.2025* | *Prima emissione* |
| | | |

# Indice

1 P1: “ANALISI DEL CONTESTO” ..... 3
2 P2: “FINALITA’ E BASE GIURIDICA” ..... 6
3 P3: “SOGGETTI COINVOLTI” ..... 8
3.1 Soggetti che trattano i dati ..... 8
3.2 Soggetti interessati di cui vengono trattati i dati ..... 8
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 ..... 12
5 P5: “DATA RETENTION” ..... 13
6 P6: “DPIA: QUANDO E PERCHE’” ..... 14
7 P7: “IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA” ..... 16
PIATTAFORMA BES ..... 16
8 P8: “ADEMPIMENTI PRIVACY” ..... 21
3. Considerazioni del Titolare del Trattamento ..... 22

# 1 P1: “ANALISI DEL CONTESTO”

| Aspetto | Risposta/Descrizione |
|---|---|
| Quali sono le **Direzioni di Regione Lombardia** coinvolte? | D.G. Università, Ricerca, Innovazione |
| Indicare il **nome dell’iniziativa/misura/servizio** | Bando “VINNOVATE OPEN CALL 2025 LOMBARDIA” |
| Fornire una descrizione testuale **dell’iniziativa/misura/servizio.** | Il Bando “VInnovate Open Call 2025 Lombardia” è una misura di Regione Lombardia attivata in sinergia con il bando congiunto interregionale VInnovate Call 2025 lanciata nell’ambito della Rete Vanguard Initiative da parte delle Regioni aderenti.<br><br>La Rete Interregionale “Vanguard Initiative – For New Growth Through Smart Specialisation” anche con l’edizione 2025 della VInnovate Call intende sostenere nell’ambito della ricerca industriale la collaborazione tra soggetti appartenenti alle regioni europee, membri della rete. In particolare, si intende favorire e consolidare la collaborazione interregionale e la capacità di realizzare progetti congiunti di ricerca industriale e sviluppo sperimentale da parte di imprese e soggetti della ricerca delle regioni aderenti.<br>Regione Lombardia in qualità di membro della Rete Vanguard Initiative aderisce in via sperimentale all’edizione 2025 della VInnovate Call.<br>Di seguito sono riportate le regioni aderenti al bando e la relativa dotazione finanziaria.<br><br>VInnovate Call 2025 - Vanguard Initiative European Regions *(amount in €)*<br>Basque Country, Spagna *(€ 250.000)*<br>East NL (Gelderland and Overijssel provinces), Paesi Bassi *(€ 750.000)*<br>Emilia-Romagna, Italia *(€ 500.000)*<br>Galicia, Spagna *(€ 1.000.000*)<br>Lombardia, Italia *(€ 250.000)*<br>Lower Austria, Austria *(€ 400.000)*<br>Lower Saxony, Germania *(€ 250.000)*<br>Noord Brabant, Paesi Bassi *(€ 250.000)*<br>Norte, Portogallo *(€ 250.000)*<br>North East Romania, Romania *(€ 1.350.000)*<br>Wales, Inghilterra *(€ 250.000)*<br>*Overall call budget (€ 5.500.000).*<br><br>I progetti interregionali devono essere presentati da un partenariato che deve essere composto da partner ammissibili provenienti da almeno due diverse regioni che hanno aderito alla VInnovate Call 2025.<br><br>Per la Lombardia, al medesimo progetto possono partecipare fino a un massimo di 2 soggetti lombardi di cui uno deve essere obbligatoriamente un’impresa (PMI) e l’altro può essere un Organismo di ricerca e diffusione della conoscenza (Università, Istituti di ricerca) pubblici o un’altra PMI. |

| | |
|---|---|
| Indicare la categoria di dati personali trattati | ☒ Dati personali comuni<br>☐ Categorie particolari di dati personali<br>☒ 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) | ARIA S.P.A. responsabile del trattamento quale gestore della piattaforma Bandi e Servizi per la finalità di raccolta e trattamento delle informazioni. |
| Indicare la **data** (anche approssimativa) di **avvio dell'iniziativa/misura/servizio** | Settembre 2025 |
| Quali sono le piattaforme informatiche che saranno utilizzate dal servizio informatico? (**esempi di piattaforme informatiche: EDMA, SIAGE, IDPC,**) | Bandi e Servizi |
| Il trattamento viene effettuato in modalità **cartacea** e/o con l'ausilio di **strumenti informatici**? | Modalità elettronica |
| 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?<br>(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 condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica della Regione Veneto, etc.) | NO |

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

Attività di raccolta, comunicazione, consultazione e conservazione dei dati ai fini dell'espletamento delle attività a partire dalla presentazione della proposta sulla piattaforma BES sino all'erogazione.

I dati saranno cancellati terminato il periodo di data retention previa comunicazione ad ARIA SPA.

**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:**<br><br>Partecipazione al Bando VInnovate Call 2025 – Lombardia e adempimenti conseguenti. | **Il trattamento in oggetto riguarda dati personali comuni ed è giustificato dalle basi giuridiche selezionate:**<br>☒Compito di interesse pubblico o connesso a esercizio di pubblici poteri del titolare<br>☐ Obbligo di legge cui è soggetto il titolare<br>☐ Interesse vitale dell'interessato o di un terzo<br>☐ Legittimo interesse del titolare o di terzi<br>☐ Adempimento di obblighi contrattuali<br>☐ Consenso<br><br>**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:**<br>☐ l'interessato ha prestato il proprio consenso esplicito<br>☐ 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<br>☐ 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;<br>☐ 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.<br>☐ il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;<br>☐ il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;<br>☐ il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri,<br>☐ 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.<br>☐ il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica.<br>☐ 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.)**<br><br>La legge regionale 23 novembre 2016, n. 29 "Lombardia è ricerca e innovazione".<br>La DCR n. XII/42/2023 approvazione del PRSS della XII Legislatura che per promuovere l'ecosistema dell'innovazione lombarda.<br>Il PST approvato con la DCR XII/613/2024.<br>La Strategia S3 2021-2027 di Regione Lombardia approvata con DGR XII/1430/2023.<br><br>**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:**<br><br>☐ condizioni relative alla liceità del trattamento<br>☐ tipologia di dati trattati<br>☐ interessati<br>☐ soggetti a cui vengono comunicati i dati<br>☐ finalità della predetta comunicazione<br>☐ limitazioni delle finalità<br>☐ periodi di conservazione<br>☐ operazioni e procedure di trattamento<br>☐ misure atte a garantire la liceità e la correttezza del trattamento<br><br>**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:**<br><br>☐ tipologia di dati trattati<br>☐ operazioni di trattamento<br>☐ motivo di interesse pubblico rilevante<br>☐ misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato |

***Nel caso di ulteriori finalità replicare le tabelle sopra riportate.**

**Eventuali note**:

_____

_____

# 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 |
|---|---|---|---|
| Partecipazione al bando da parte di PMI e OdR | Regione Lombardia | Aria S.p.A. | INPS, INAIL, Camere di Commercio, Ministero delle Imprese e del Made in Italy per il caricamento delle informazioni nel Registro Nazionale degli Aiuti di Stato (RNA), Ministero della Giustizia e i Comuni. |

## 3.2 Soggetti interessati di cui vengono trattati i dati

| Aspetto | Risposta/Descrizione |
|---|---|
| Qual è la **tipologia di soggetti interessati coinvolti?** | I titolari di imprese individuali e i titolari effettivi (ai fini della normativa antiriciclaggio) delle PMI, i legali rappresentanti e i delegati della PMI o OdR.<br>I Responsabili scientifici e i Responsabili amministrativi del Progetto di PMI e OdR.<br>I componenti del Nucleo di Valutazione interno (3 membri). |
| Fornire una stima del **numero di soggetti interessati coinvolti** | Massimo 30 |

**Eventuali note**:

_____
_____
_____
_____

# 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**<br>☒Dati identificativi diretti<br>☒Dati identificativi indiretti<br>☐Stato civile<br>☐Percorso professionale<br>☐Dati di connettività<br>☒Altro<br>Iban (imprese individuali<br><br>**Dati personali comuni percepiti come critici**<br>☐Dati riguardanti la vita privata<br>☐Informazioni finanziarie<br>☐Dati identificativi di conti correnti, carte di debito, credito, etc.<br>☐Dati sulla posizione<br>☐Altro<br><br>**Categorie particolari di dati personali / Dati personali relativi a condanne penali o reati**<br>☐Dati relativi alla salute<br>☐Dati relativi alla vita sessuale | Per i titolari di imprese individuali e i titolari effettivi (ai fini della normativa antiriciclaggio) delle PMI, i rappresentanti legali e i delegati delle imprese PMI e degli Organismi di Ricerca:<br>· Nome<br>· Cognome<br>· Data e luogo di nascita<br>· Codice fiscale<br>· Documento di riconoscimento<br>· Telefono<br>· E-mail/PEC<br><br>Per i Responsabili scientifici e i Responsabili amministrativi del Progetto di PMI e OdR:<br>· Nome<br>· Cognome<br>· Telefono/E-mail | I dati trattati sono limitati, adeguati e pertinenti rispetto alle finalità?<br><br>Per ciascuna categoria/dato giustificare il motivo per il quale il dato è trattato. | SI<br><br>Nome, cognome, data e luogo di nascita, codice fiscale e documento di riconoscimento sono necessari per individuare in modo univoco ciascun soggetto.<br><br>Il telefono e l'indirizzo e-mail/pec sono necessari per inviare comunicazioni agli interessati.<br><br>Il curriculum vitae è necessario per valutare l'idoneità dei componenti del Nucleo di Valutazione.<br><br>I dati relativi a condanne penali sono necessari ai fini della nomina dei componenti del Nucleo di Valutazione.<br><br>L'Iban è necessario per l'erogazione alle imprese individuali. |

| 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 relativi all'orientamento sessuale<br>☐Dati biometrici<br>☐Dati genetici<br>☐Convinzioni religiose o filosofiche<br>☐Dati che rivelino l'origine razziale o etnica<br>☐Dati sull'appartenenza sindacale<br>☒Dati relativi a condanne penali<br>☐Dati riguardanti reati<br>☐Altro | Per i componenti del Nucleo di Valutazione interno:<br>· Nome<br>· Cognome<br>· Codice fiscale<br>· Data e luogo di nascita<br>· Comune di residenza<br>· Curruculum vitae<br>· Telefono/E-mail<br>· Dati relativi a condanne penali e reati | | |
| | | **Nel caso in cui vengano trattate categorie particolari di dati personali, è possibile evitarne il trattamento? Motivare la risposta** | |
| | | | - |

**Eventuali note**: i dati particolari si riferiscono ai componenti del Nucleo di valutazione.

## 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<br>☒Consultazione<br>☐Pubblicazione<br>☒Raccolta<br>☐Elaborazione<br>☒Conservazione<br>☐Interconnessione<br>☒Altro (specificare)<br>Cancellazione<br><br>Indicare se i dati vengono raccolti:<br>☒Direttamente dall'interessato (es. compilazione di un form su una pagina web, compilazione di una scheda di raccolta cartacea, etc.)<br>☒Indirettamente (es. ottenimento di dati personali da terzi): indicazione dei referenti operativi. | **Tutte le operazioni sui dati indicate sono necessarie per il raggiungimento della finalità del trattamento?**<br>**Per ciascuna operazione giustificare per quale motivo viene svolta. Evitare operazioni non necessarie rispetto alle finalità.** | SI<br><br>La raccolta è necessaria per l'acquisizione dei dati.<br>La comunicazione dei dati agli Enti Comunali e al Ministero della Giustizia è necessaria per la verifica delle condanne penali dei componenti del Nucleo di valutazione.<br>La consultazione è necessaria per la verifica dei dati.<br>La conservazione è necessaria per l'espletamento di eventuali successive attività di controllo.<br>La cancellazione è effettuata quando non vi è più necessità di trattamento. |
| | **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**<br>☒Soggetti appartenenti alla DG Università, Ricerca, Innovazione<br>☐Soggetti della funzione sistemi informativi<br>☐Soggetti delle funzioni di audit e compliance | **Per ciascuna tipologia di utenti che accede ai dati personali indicare il motivo per il quale è concesso l'accesso.** | L'accesso dei dati da parte dei soggetti appartenenti alla DG Università, Ricerca, Innovazione è finalizzato all'attuazione del Bando. |
| | **Soggetti esterni autorizzati**<br>☒ Funzioni di help desk<br>☒ Funzioni di supporto sistemistico<br>☐Dipendenti di enti pubblici es. Comuni, Ministeri etc. (specificare ente di appartenenza)<br>☒Altri soggetti di altre società esterne (Aria S.p.A) | **L'accesso è necessario/limitato rispetto alle attività che devono essere svolte?**<br>**Per ciascuna tipologia di utenti sono stati stabiliti i privilegi di accesso?**<br>**I privilegi di accesso sono necessari/limitati rispetto alle attività che devono essere svolte?** | L'accesso ai dati da parte dei soggetti appartenenti alla DG è necessario e limitato rispetto alle sole attività che devono essere svolte per l'attuazione del bando<br>SI<br>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** | 5 anni dalla data dell’ultima liquidazione | Il tempo di data retention tiene conto del periodo massimo per le restituzioni di cui all’art 65 “Stabilità delle operazioni” del Reg. UE n. 2021/1060 (Disposizioni comuni applicabili al Fondo europeo di sviluppo regionale) del 24 giugno 2021 e s.m.i. |

**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). | NO |
| **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. | NO |
| **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 P7: "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<br>☐No |
| **È stata già svolta un'analisi dei Rischi sul servizio da parte del fornitore (es: Aria)?** | ☒Sì<br>☐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<br>☐ In parte<br>☐ No<br>☐ 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<br>☐ In parte<br>☐ No<br>☐ N/A | …… |

| Area | Misura di sicurezza | Livello di implementazione | Note di commento e approfondimento |
|---|---|---|---|
| **Access Management** | **È previsto che le utenze abilitate ad accedere al sistema vengano create, modificate, riviste e cancellate,** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| | **È previsto che l'accesso al sistema avvenga attraverso una combinazione di username e password?** | ☐ Si<br>☒ In parte<br>☐ No<br>☐ N/A | A seguito del DL "semplificazione e innovazione digitale" del 28 febbraio 2021 e s.m.i. è consentito l'accesso tramite username e password solo per cittadini NON in possesso di documento di identità riconosciuto dallo Stato italiano |
| | **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<br>☐ In parte<br>☐ No<br>☐ N/A | …… |

| 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<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| | **È previsto che per l'accesso ai sistemi venga richiesto un sistema di multi factor authentication?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ N/A | |
| **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<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| | **È previsto che i file di log siano adeguatamente protetti da manomissioni e accessi non autorizzati?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| | **È previsto che le attività degli amministratori di sistema vengano registrate, analizzate e riviste periodicamente?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ 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<br>☒ In parte<br>☐ No<br>☐ 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<br>☐ In parte<br>☐ No<br>☐ N/A | Utilizzo di canali sicuri (HTTPS e firewall) |
| **Sicurezza delle applicazioni** | **È prevista, per il servizio, l'esecuzione di attività di Vulnerability assessment e Penetration test?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ 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<br>☐ In parte<br>☐ No<br>☐ 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<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| | **È previsto che l'esecuzione del backup del sistema venga monitorato?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| | **È previsto vengano effettuati test periodici di Restore del Backup e test del Disaster Recovery?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ 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<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| | **È previsto che in caso di Data Breach venga seguita la procedura di Data Breach definita dall'organizzazione?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ 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<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| **Sicurezza fisica** | **È prevista l'applicazione di adeguate misure di sicurezza fisica presso le aree critiche (e.g. sale CED)?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ N/A | …… |
| **Gestione del Rischio** | **È prevista l'esecuzione dell'analisi dei Rischi IT per il servizio da parte del fornitore?** | ☒ Si<br>☐ In parte<br>☐ No<br>☐ 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<br>☐ In parte<br>☐ No<br>☐ 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<br>☐ In parte<br>☐ No<br>☒ N/A | Non è previsto l'utilizzo di dati cartacei |

# 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:

| |
|---|
| L’informativa sarà pubblicata in BES |

.☒ 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**:
_____
_____
_____
_____

# 3. Considerazioni del Titolare del Trattamento

La sottoscritta Elisabetta Confalonieri in qualità di Direttore Generale della Direzione Università, Ricerca, Innovazione 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 e di aver aggiornato il registro dei trattamenti.

Di aver aggiornato il registro dei trattamenti.

È stato compilato il seguente documento:

- **VERBALE - PRIVACY BY DESIGN**

**Privacy Officer:** Dr. Gianluca Jesu

**EQ competente per il procedimento:** Dott.ssa Vincenzina Cristofaro

**Dirigente referente privacy:** Dr. Tommaso Mazzei

**EQ referente privacy:** Dott.ssa Carla Recchia

**EQ referente sistemi informativi:** Dott.ssa Silvia Eugenia Ronzio

**Aria S.p.A** – Dr. Angelo Nitti

**Per la Direzione Università, Ricerca, Innovazione** Il Direttore Dott.ssa Elisabetta Confalonieri