Verbale

“Privacy By design”

MISURA PER IL RAFFORZAMENTO DELLE FILIERE PRODUTTIVE E DEGLI ECOSISTEMI INDUSTRIALI - 2025

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

Revisione	Data	Sintesi delle Modifiche
0	10/02/2024	Prima emissione
1	10/03/2025	Prima revisione

Indice

1 P1: “ANALISI DEL CONTESTO”

Aspetto	Risposta/Descrizione
Quali sono le **Direzioni di Regione Lombardia** coinvolte?	Direzione Generale Sviluppo Economico
Indicare il **nome dell'iniziativa/misura/servizio**	**MISURA PER IL RAFFORZAMENTO DELLE FILIERE PRODUTTIVE E DEGLI ECOSISTEMI INDUSTRIALI 2025**
Fornire una descrizione testuale **dell'iniziativa/misura/servizio.**	La Misura sostiene il rafforzamento delle filiere produttive e degli ecosistemi industriali regionali (nelle catene globali del valore) per accrescere, anche in coerenza con la strategia industriale UE, la capacità di innovazione, produzione e investimento delle imprese e, in particolare, le PMI. Nello specifico, la Misura riguarda l'innovazione, il miglioramento tecnologico e il rafforzamento competitivo delle filiere e degli ecosistemi industriali, nonché il sostegno alla costituzione e allo sviluppo di nuove filiere attraverso la realizzazione di progetti di filiera, anche integrati con attività di sviluppo sperimentale svolta da una impresa facente parte della filiera
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)	ARIA S.p.A. FINLOMBARDA S.p.A.
Indicare la **data** (anche approssimativa) di **avvio dell'iniziativa/misura/servizio**	aprile 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**?	SOLO INFORMATICI
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 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.

I dati vengono raccolti mediante inserimento in BES da parte dell'impresa capofila di ciascun raggruppamento di filiera e riguardano i dati personali dei delegati e dei professionisti individuati dalle imprese; i dati vengono consultati per l'istruttoria formale, tecnica economico-finanziaria e di merito sia dal personale regionale (max 10 persone) sia dagli operatori di FL che opera in qualità di soggetto gestore per l'azione 1.3.4. (contributo + finanziamento) e in qualità di Organismo Intermedio per l'azione 1.1.1. (contributo). Questi dati verranno cancellati a partire dal 10 anno successivo alla data concessione dell'agevolazione in ragione della norma sugli aiuti di stato.

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: Concedere agevolazioni a raggruppamenti di imprese in filiera (PMI, Midcap, grande impresa) che presentino progetti ammissibili secondo i criteri del bando **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.)** **Regolamento (UE) n. 2021/1060 del Parlamento europeo e del Consiglio del 24 giugno 2021 recante le disposizioni comuni applicabili al Fondo europeo di sviluppo regionale (FESR), al Fondo sociale europeo Plus (FSE+), al Fondo di coesione, al Fondo per una transizione giusta (JTF), al Fondo europeo per gli affari marittimi, la pesca e l'acquacoltura (FEAMPA) e le regole finanziarie applicabili.** **L.r. 11/2014 art. 5-bis** **Atti di normazione secondaria e delibere di giunta regionale** **D.g.r. 6884/2022 presa d’atto della decisione di esecuzione della Commissione Europea C(2022) 5671 final del 01.08.22 di approvazione del PR-FESR 2021-2027** **DGR n. 3703 del 20.12.2024 2021IT16RFPR010 – Nuove determinazioni sulla misura per il rafforzamento delle filiere produttive e degli ecosistemi industriali a valere sulle azioni 1.3.4. “Sostegno al rafforzamento delle reti e delle aggregazioni di imprese” e 1.1.1. “Sostegno agli investimenti in ricerca, sviluppo e innovazione” del PR FESR Lombardia 2021-2027 e approvazione dei criteri applicativi 2025 “ (ed 2025)** **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

***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
Concedere agevolazioni a raggruppamenti di imprese in filiera (PMI, Midcap, grande impresa) che presentino progetti ammissibili secondo i criteri del bando	Regione Lombardia	Finlombarda S.p.A. ARIA S.p.A.	

3.2 Soggetti interessati di cui vengono trattati i dati

Aspetto	Risposta/Descrizione
Qual è la **tipologia di soggetti interessati coinvolti?**	Persone fisiche delegate dal rappresentante legale; titolare di ditta individuale; personale tecnico scientifico individuato dalle imprese
Fornire una stima del **numero di soggetti interessati coinvolti**	30 (3 persone per un massimo di 10 filiere nell’arco del settennio di apertura del fondo)

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 ☒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	**Nome cognome e C.F. dei delegati; nome, cognome, e-mail per il personale tecnico-scientifico delle imprese e percorso professionale**	**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 sono richiesti per identificare la persona fisica;** **i dati professionali richiesti sono quelli dei professionisti, al fine di avvalorare la scelta operata dall'impresa rispetto ai collaboratori professionisti per lo sviluppo sperimentale della progettualità**

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 per sonali 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		**Nel caso in cui vengano trattate categorie particolari di dati personali, è possibile evitarne il trattamento? motivare la risposta**	-
			-

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.** **Vi è una pubblicazione o diffusione di dati personali? A quale scopo? Risulta applicabile/da applicare il principio di trasparenza?** **È necessario realizzare copie dei dati personali (esempio: copie dell'archivio)? motivare la risposta**	si Raccolte e consultate per l'identificazione dell'interessato in fase di istruttoria, concessione ed erogazione. Conservate per eventuali verifiche e controlli ex post successivi alla concessione dell'agevolazione. No no
	Le operazioni indicate includono l'impiego di algoritmi decisionali/trattamenti automatizzati che producono effetti giuridici sugli interessati? **Viene effettuata profilazione?**	no 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 alla DG ☒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. (specificare ente di appartenenza) ☒Altri soggetti di altre società esterne Finlombarda S.p.A.	**Per ciascuna tipologia di utenti che accede ai dati personali indicare il motivo per il quale è concesso l'accesso.** **L'accesso è necessario/limitato rispetto alle attività che devono essere svolte?** **Per ciascuna tipologia di utenti sono stati stabiliti i privilegi di accesso?** **I privilegi di accesso sono necessari/limitati rispetto alle attività che devono essere svolte?**	**Personale della DG: motivi istruttori** **Sistemi informativi: in caso di problemi tecnico informatici di sistema** **Audit e compliance: per i controlli** **Si** **si** **si** **i soggetti esterni sono quelli autorizzati da FL che opera in qualità di Soggetto Gestore/O.I.**

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	10 anni a partire dall’anno successivo alla data di concessione dell’agevolazione.	Art. 4 del DM 31maggio 2017 n. 115 e art 52 legge 234 del 2012 istitutiva del registro aiuti di stato

Eventuali note:

l’art. 4 del d.m. 31 maggio 2017, n. 115 “*Regolamento recante la disciplina per il funzionamento del Registro nazionale degli aiuti di Stato, ai sensi dell'articolo 52, comma 6, della legge 24 dicembre 2012, n. 234 e successive modifiche e integrazioni*” che riporta quanto segue:

“Le informazioni e i dati presenti nel Registro nazionale aiuti, ai sensi dell'articolo 52, comma 4, della legge 24 dicembre 2012, n. 234 “, sono conservati e resi accessibili per almeno dieci anni dalla data di concessione dell'aiuto”

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"

7.1 Piattaforma Bandi e Servizi

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 dall'ambiente di produzione?	☒ Si ☐ In parte ☐ No ☐ 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 ☐ 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	A seguito del DL Semplificazione 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 ☐ In parte ☐ No ☐ N/A	……
	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	……

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	……
	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	È previsto un rilascio nel 2025 per applicare tecniche di pseudonimizzazione in funzione dei dati trattati, mediante la configurazione degli strumenti attuativi in bandi e Servizi. In attesa del rilascio è possibile individuare i dati personali/sensibili direttamente nell'ambiente di progettazione di bandi e servizi e applicare una procedura di pseudonimizzazione tramite l'intervento del gestore del servizio.

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	Non è previsto l'utilizzo dei dati in formato cartaceo

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:

Attraverso la pubblicazione in Bandi e Servizi nello spazio dedicato alla misura e allegata al bando, pubblicato sia in BURL che in Bandi e Servizi, sul sito istituzionale di RL, sul sito dedicato al PR-FESR di Regione Lombardia e sul sito istituzionale di FL

☒ 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

Il sottoscritto Armando De Crinito in qualità di Direttore Generale della Direzione Generale Sviluppo Economico 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.

Sono stati compilati i documenti:

- VERBALE - PRIVACY BY DESIGN

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

Privacy Officer:

Dr. Gianluca Jesu

Per la Direzione Generale Sviluppo Economico:

Dr. Armando De Crinito

Dirigente responsabile del procedimento Carlo Bianchessi

PO competente per il procedimento Veronica Redaelli

Dirigente referente privacy Armando de Crinito

PO referente privacy Valeria La Paglia

Service manager ARIA S.p.A. Maurizio De Bartolo

FINLOMBARDA: Paola Peduzzi