

Verbale

“Privacy By design e DPIA”

< **Bando Ri.Circo.Lo. Risorse Circolari in Lombardia per il sostegno alle PMI lombarde per lo sviluppo di azioni di economia circolare. Edizione dedicata alle filiere della plastica e del tessile.**

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

Revisione	Data	Sintesi delle Modifiche
1	26.03.2024	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	12
5 P5: “DATA RETENTION”	13
6 P6: “DPIA: QUANDO E PERCHE’”	14
7 P7: “IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA”	16
8 P8: “ADEMPIMENTI PRIVACY”	21
Allegato 1: “ANALISI INTEGRATIVA PER TRATTAMENTI DA SOTTOPORRE A DPIA”	Errore. Il segnalibro non è definito.
1. Valutazioni giuridiche	Errore. Il segnalibro non è definito.
1.1 Valutazioni sul rispetto del principio di trasparenza	Errore. Il segnalibro non è definito.
1.2 Valutazioni sul rispetto del principio di accuratezza	Errore. Il segnalibro non è definito.
1.3 Valutazioni sul rispetto dei diritti e delle libertà fondamentali della persona	Errore. Il segnalibro non è definito.
1.4 Diritti esercitabili dall’interessato	Errore. Il segnalibro non è definito.
1.5 Valutazione dei rischi per i diritti e le libertà degli interessati – rischio informatico	Errore. Il segnalibro non è definito.
1.6 Valutazione giuridica finale sul trattamento	Errore. Il segnalibro non è definito.
2. Valutazioni in materia di sicurezza	Errore. Il segnalibro non è definito.
3. Considerazioni del Titolare del Trattamento	Errore. Il segnalibro non è definito.
4. Considerazioni finali del DPO	Errore. Il segnalibro non è definito.

1 P1: “ANALISI DEL CONTESTO”

Aspetto	Risposta/Descrizione
Quali sono le Direzioni di Regione Lombardia coinvolte?	Direzione Generale Ambiente e Clima
Indicare il nome dell'iniziativa/misura/servizio	Bando Ri.Circo.Lo. Risorse Circolari in Lombardia per il sostegno alle PMI lombarde per lo sviluppo di azioni di economia circolare. Edizione dedicata alle filiere della plastica e del tessile. (PR FESR Regione Lombardia 2021-2027 – asse 2: azione 2.6.2.)
Fornire una descrizione testuale dell'iniziativa/misura/servizio .	Il bando, attraverso l'erogazione di finanziamenti pubblici, in attuazione del PR FESR Regione Lombardia 2021-2027 – asse 2: azione 2.6.2., promuove azioni di economia circolare da parte delle PMI lombarde per conseguire la riduzione ed una migliore gestione dei rifiuti delle filiere delle plastiche e del tessile. Inoltre, il bando attua l'obiettivo del PRSS 5.1.4 “Sviluppare sul territorio l'economia circolare”. La domanda di partecipazione deve essere presentata in forma telematica per mezzo di Bandi e Servizi (www.bandi.regione.lombardia.it).
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 con Bandi e Servizi
Indicare la data (anche approssimativa) di avvio dell'iniziativa/misura/servizio	L'apertura del bando è prevista a maggio 2024

Quali sono le piattaforme informatiche che saranno utilizzate dal servizio informatico? (esempi di piattaforme informatiche: EDMA, SIAGE, IDPC,)	Bandi e Servizi Edma Sap per l'erogazione dei contributi
Il trattamento viene effettuato in modalità cartacea e/o con l'ausilio di strumenti informatici ?	Solo con l'ausilio di strumenti 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.	

1. Vengono raccolti i dati personali al momento della presentazione della domanda su BeS;
2. I dati vengono trattati per istruire la domanda e assegnare il contributo;
3. I dati sono necessari per la verifica dei dati economici legati alla rendicontazione e all'erogazione e del contributo e per l'esecuzione dei controlli a campione previsti per legge sulle autodichiarazioni rilasciate ai fini della partecipazione al bando.

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 normale si fonda il trattamento?
Finalità 1: Istruttoria amministrativa sull'ammissibilità delle domande finalizzate all'erogazione del contributo e l'attuazione dei controlli dovuti 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 persegue 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 esercitano 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.) - Art. 6 lett. e) GDPR (“esecuzione di un compito di interesse pubblico e/o connesso all'esercizio di pubblici poteri”) - Art. 2, ter del d.lgs. 196/2003 e s.m.i. - D.lgs. 3 aprile 2006, n. 152/2006 “Norme in materia ambientale” Atti di normazione secondaria e delibere di giunta regionale - D.g.r. n. XI/6884/2022 presa d'atto dell'approvazione da parte della Commissione Europea del programma regionale PR FESR 2021-2027 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
Istruttoria amministrativa sull'ammissibilità delle domande finalizzate all'erogazione del contributo e l'attuazione dei controlli dovuti	Regione Lombardia	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 ?	Imprese individuali e contatti dei referenti delle PMI
Fornire una stima del numero di soggetti interessati coinvolti	40/50 imprese con team presumibilmente di 10/15 persone per impresa

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 Dati personali dei familiari (informativa antimafia) 	1) Nome e cognome, codice fiscale, telefono, indirizzo mail. 2) Dati personali dei familiari 3) IBAN 4) Specificazione del genere e/o dell'età dei partecipanti al team 5) Documento di identità.	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.	Sì 1) Necessità di contattare le imprese 2) Per effettuare i controlli previsti per legge (informativa antimafia) 3) Per l'erogazione del contributo 4) Per la valutazione della concessione delle premialità viene richiesta la dichiarazione di rilevanza della componente femminile nel team e/o la rilevanza della componente giovanile 5) Per consentire sottoscrizione per conto del legale rappresentante o per presentazione di fidejussione.

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) 	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	Consultazione per l'espletamento dell'istruttoria. Raccolta per l'espletamento dell'istruttoria Conservazione per i controlli successivi no no
Indicare se i dati vengono raccolti: ☒ Direttamente (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) Capofila di aggregazioni di imprese Dati dei partecipanti ai team di progetto	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 dei dati 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 (ARIA spa)	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?	5 funzionari della U.O. Economia Circolare e tutela delle risorse naturali per prendere in carico le domande, effettuare l'istruttoria 5 funzionari della U.O. Economia Circolare e tutela delle risorse naturali per i controlli ed erogare i contributi Le regole PR FESR prevedono la separazione delle due funzioni. Sì Team per il supporto help desk (ARIA SpA) Team per il supporto sistemistico (ARIA SpA) Sì

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
		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 sì indicare quale Altrimenti fornire il criterio utilizzato per determinarlo
Dati dell'iniziativa/misura/servizio che stai considerando	10 anni	10 Anni dalla data di approvazione del decreto di erogazione del saldo di ciascuna domanda in quanto si tratta di fondi comunitari, per garantire i controlli post erogazione (ex art. 2220 cod. civ) e per i controlli previsti dal Regolamento Europeo n.1060/2021

Eventuali note:

6 P6: “DPIA: QUANDO E PERCHE”

<i>L'iniziativa/misura/servizio ricade in uno di questi casi?</i>	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 <i>“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”</i> .	no
Trattamenti automatizzati finalizzati ad assumere decisioni che producono <i>“effetti giuridici”</i> oppure che incidono <i>“in modo analogo significativamente”</i> 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. <i>screening</i> 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 <i>budget</i> , di <i>upgrade</i> 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 <i>wearable</i> ; tracciamenti di prossimità come ad es. il <i>wi-fi tracking</i>) 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. <i>mobile payment</i>).	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”

Per 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 (“Sì” 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?	☒ Sì ☐ 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?	☒ Sì ☐ 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,	☒ Sì ☐ In parte ☐ No ☐ N/A	
	È previsto che l'accesso al sistema avvenga attraverso una combinazione di username e password?	☐ Sì ☒ 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?	☒ Sì ☐ 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)?	☒ Sì ☐ In parte ☐ No ☐ N/A	
	È previsto che per l'accesso ai sistemi venga richiesto un sistema di multi factor authentication?	☒ Sì ☐ In parte ☐ No ☐ N/A	SPID livello 2, CIE, CNS

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?	☒ Sì ☐ In parte ☐ No ☐ N/A	
	È previsto che i file di log siano adeguatamente protetti da manomissioni e accessi non autorizzati?	☒ Sì ☐ In parte ☐ No ☐ N/A	
	È previsto che le attività degli amministratori di sistema vengano registrate, analizzate e rivate periodicamente?	☒ Sì ☐ 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?	☒ Sì ☐ In parte ☐ No ☐ N/A	E' previsto un rilascio nel primo semestre del 2024 per applicare tecniche di pseudonimizzazione in funzione dei dati trattati, mediante la configurazione degli strumenti attuativi in Bandi online. In attesa del rilascio è possibile già oggi individuare i dati personali direttamente nell'ambiente di progettazione di Bandi online 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)?	☒ Sì ☐ In parte ☐ No ☐ 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?	☒ Sì ☐ 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?	☒ Sì ☐ 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?	☒ Sì ☐ In parte ☐ No ☐ N/A	
	È previsto che l'esecuzione del backup del sistema venga monitorato?	☒ Sì ☐ In parte ☐ No ☐ N/A	
	È previsto vengano effettuati test periodici di Restore del Backup e test del Disaster Recovery?	☒ Sì ☐ 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?	☒ Sì ☐ In parte ☐ No ☐ N/A	
	È previsto che in caso di Data Breach venga seguita la procedura di Data Breach definita dall'organizzazione?	☒ Sì ☐ 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?	☒ Sì ☐ 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)?	☒ Sì ☐ In parte ☐ No ☐ N/A	
Gestione del Rischio	È prevista l'esecuzione dell'analisi dei Rischi IT per il servizio da parte del fornitore?	☒ Sì ☐ 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?	☒ Sì ☐ 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?	☐ Sì ☐ In parte ☐ No ☒ 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:

Caricamento su BeS con la funzione di flag per presa visione e pubblicazione sul burl quale allegato al decreto di approvazione del bando.

- ☒ 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:

Privacy Officer:

Dr. Gianluca Jesu

Per la Direzione Ambiente e Clima:

Dr. Dario Fossati

Dirigente responsabile del procedimento Giorgio Gallina

PO competente per il procedimento Silvia Passoni

Dirigente referente privacy Enrica Mainardi

PO referente privacy Elena Colao

Responsabile del trattamento per ARIA: De Bartolo Maurizio