Verbale

“Privacy By design e DPIA”

PROCEDIMENTO UNICO CENTRI DATI

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

Revisione	Data	Sintesi delle Modifiche
1	*23/06/2026*	*Prima emissione*

Indice

1 P1: “ANALISI DEL CONTESTO” 3
2 P2: “FINALITA’ E BASE GIURIDICA” 7
3 P3: “SOGGETTI COINVOLTI” 9
3.1 Soggetti che trattano i dati 9
3.2 Soggetti interessati di cui vengono trattati i dati 10
4 P4: “VALUTAZIONE DI NECESSITA’ E PROPORZIONALITA’” 11
4.1 Dati personali trattati 11
4.2 Operazioni sui dati 13
4.3 Accesso ai dati personali 14
5 P5: “DATA RETENTION” 16
6 P6: “DPIA: QUANDO E PERCHE’” 17
7 P7: “IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA” 19
8 P8: “ADEMPIMENTI PRIVACY” 24
3. Considerazioni del Titolare del Trattamento 30

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**	Procedimento unico per il rilascio delle autorizzazioni ai progetti di centri dati
Fornire una descrizione testuale **dell’iniziativa/misura/servizio.**	Il nuovo “Procedimento unico per il rilascio delle autorizzazioni ai progetti di centri dati”, introdotto dall’art. 8 del Decreto-Legge 20 febbraio 2026, n. 21, convertito con modificazioni dalla L. 10 aprile 2026, n. 49, riguarda l’ *“autorizzazione per la realizzazione, l'ampliamento e l'esercizio dei centri dati*”, consentendo la possibilità di raccogliere le principali informazioni contenute nelle istanze (anagrafica, certificazioni ambientali, dati progettuali, dati emissivi), e di agevolare – contestualmente - gli utenti nella compilazione delle istanze.
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. Responsabile del trattamento Engineering (sub-responsabile nominato da Aria S.p.A.). Business Changers (sub-responsabile nominato da Aria S.p.A.). Business Integration Partner (sub-responsabile nominato da Aria S.p.A.). In qualità di titolari autonomi: Prefetture MASE Province

	Città Metropolitana di Milano Comuni ARPA Lombardia Autorità d'Ambito Gestore del Servizio Idrico Integrato Sovrintendenza dei Beni Ambientali e del Paesaggio ATS Comunità Montane Enti Parco Vigili del Fuoco Gestori di servizi di rete TERNA
Indicare la **data** (anche approssimativa) di **avvio dell'iniziativa/misura/servizio**	1 Settembre 2026
Quali sono le piattaforme informatiche che saranno utilizzate dal servizio informatico? (**esempi di piattaforme informatiche: EDMA, SIAGE, IDPC,**)	Bandi e Servizi EDMA BDNA (Banca dati nazionale antimafia)
Il trattamento viene effettuato in modalità **cartacea** e/o con l'ausilio di **strumenti informatici**?	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. Regione Lombardia in qualità di Autorità competente gestisce attraverso la piattaforma l'intero iter istruttorio, comprendente: la verifica formale della documentazione e la protocollazione della pratica; la richiesta di integrazioni documentali o pareri a enti terzi; la convocazione e gestione delle Conferenze di Servizi, con la possibilità di allegare i verbali firmati digitalmente; la conclusione del procedimento con il rilascio o il diniego dell'autorizzazione unica.
2. I dati personali dei legali rappresentanti o eventuali delegati vengono raccolti al momento della presentazione dell'istanza su BeS, comprensiva di tutta la documentazione tecnica ed elaborati progettuali previsti dalle normative di settore, per consentire la compiuta istruttoria tecnico-amministrativa finalizzata al rilascio di tutte le autorizzazioni, intese, licenze, pareri, concerti, nulla osta e assensi comunque denominati, compresi quelli per l'autorizzazione integrata ambientale, la valutazione di impatto ambientale, l'autorizzazione paesaggistica o culturale, per l'utilizzo delle acque ovvero per le emissioni atmosferiche, ivi compresa la verifica di conformità urbanistica ai piani comunali, necessari alla realizzazione e all'esercizio del medesimo progetto, nonché copia dell'avvenuto pagamento degli oneri istruttori.
3. Durante la compilazione vengono inseriti nell'applicativo: dati anagrafici e di contatto del titolare gestore dell'impianto (se diverso dal legale rappresentante) o del delegato e del referente IPPC.
4. Vengono raccolti anche i dati dei progettisti/professionisti che redigono i documenti necessari alla presentazione dell'istanza.
5. I dati personali dei legali rappresentanti, amministratori, i soci e familiari conviventi sono comunicati agli uffici delle prefetture competenti per i controlli sulle cause di divieto, di decadenza, di sospensione previste dall'art. 67 D.lgs. 6 settembre 2011, n.159 (Codice antimafia).
6. La piattaforma è accessibile, mediante abilitazione, ai titolari autonomi del Trattamento, quali amministrazioni pubbliche (Province e Città Metropolitana di Milano, Comuni) ed Enti (ARPA, Comunità Montane, Enti Parco, VVF, TERNA…) destinatari dei vari titoli che confluiscono nel PROCEDIMENTO UNICO CENTRI DATI in funzione delle relative competenze. I dati vengono trattati esclusivamente per finalità istruttorie e di verifica tecnica, urbanistica e ambientale da parte dei referenti degli Enti/amministrazioni che accedono all'applicativo previa profilazione. Tutte le attività e gli accessi sono registrati nei log di audit gestiti da ARIA S.p.A., che riportano data, ora, utente e operazione effettuata.

7. L'amministrazione conserva i dati personali secondo i termini previsti nella data retention. I dati e i documenti raccolti sono conservati per 30 anni a decorrere dal rilascio dell'autorizzazione per: - la validità giuridico-amministrativa del procedimento durante il ciclo di vita dell'impianto; - le verifiche e controlli successivi da parte di organi di audit, vigilanza o giurisdizionali.
8. Regione Lombardia, quale Autorità competente per il Procedimento Unico di cui all'art. 8 del DL 21/2026, pubblica sul proprio sito web, in attuazione dell'art. 29quater c.3 del d.lgs 152/2006 e dell'art. 4 c.9 della LR 11/2026, un report/sintesi relativo al procedimento in questione comprensivo delle informazioni relative alle varie fasi procedurali necessarie, omettendo eventuali dati personali.
9. Il pubblico può presentare osservazioni inviando il modulo, comprensivo di apposita informativa privacy, dichiarando i propri dati personali. Il modulo è messo a disposizione nella sezione del sito di Regione Lombardia dedicata al Procedimento Unico Data Center, e andrà inviato a mezzo PEC all'indirizzo ambiente_clima@pec.regione.lombardia.it;
10. I tempi di conservazione dei dati personali previsti per l'ulteriore finalità di archiviazione dei documenti ai sensi di quanto indicato dalla normativa di riferimento e conformemente a quanto previsto dal «Aggiornamento Titolario di classificazione e Massimario di scarto dei documenti digitali ed analogici di Giunta Regionale» approvato con Decreto n. 4413 del 7 aprile 2026 e s.m.i.
11. I dati personali vengono cancellati o anonimizzati, in conformità alla normativa sulla protezione dei dati personali (Reg. UE 2016/679 e D.Lgs. 196/2003). Le operazioni di cancellazione sono eseguite da ARIA S.p.A., quale Responsabile del trattamento.

Eventuali note: Il servizio realizza la completa informatizzazione del processo, dalla presentazione dell'istanza all'autorizzazione da parte dell'autorità compente.

Il provvedimento finale del PROCEDIMENTO UNICO CENTRI DATI varrà come autorizzazione per la realizzazione, l'ampliamento e l'esercizio dei centri dati, includendo l'Autorizzazione Integrata Ambientale (AIA), la Valutazione di Impatto Ambientale (VIA o verifica di VIA) di competenza ministeriale e gli altri titoli autorizzativi/abilitativi previsti dalla normativa di settore.

I vari titoli, esplicitamente individuati e richiesti dal Proponente nell'istanza presentata ai sensi dell'art.8 c.3 del DL 21/2026, che confluiscono nel PROCEDIMENTO UNICO CENTRI DATI, dovranno essere acquisiti da parte dell'Autorità competente al rilascio dell'autorizzazione unica, dai rispettivi Enti/Amministrazioni competenti; questi ultimi dovranno fornire le rispettive determinazioni in sede di Conferenza dei servizi.

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: Istruttoria amministrativa finalizzata al rilascio dell’autorizzazione riferita al procedimento unico centri dati **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.)** - 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.152/2006 (Codice dell’Ambiente) - il Decreto-Legge 20 febbraio 2026, n. 21 convertito con modificazioni dalla L. 10 aprile 2026, n. 49, in particolare l’art. 8 che ha introdotto il “Procedimento unico per il rilascio delle autorizzazioni ai progetti di centri dati” - la Legge regionale 3 giugno 2026 - n. 11 “Disposizioni in materia di insediamento di centri dati” - Art. 67 D.lgs. 6 settembre 2011, n.159 (Codice antimafia) **Atti di normazione secondaria e delibere di giunta regionale** - DELIBERAZIONI N. XII/ 6645 E XII/ 6646 del 03/08/26 **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

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
Istruttoria amministrativa finalizzata al rilascio dell’autorizzazione riferita al procedimento unico centri dati	Regione Lombardia	Aria S.p.a. Engineering (sub-responsabile nominato da Aria S.p.A.). Business Changers (sub-responsabile nominato da Aria S.p.A.). Business Integration Partner (sub-responsabile nominato da Aria S.p.A.).	Prefetture MASE Province Città Metropolitana di Milano Comuni ARPA Lombardia Autorità d’Ambito Gestore del Servizio Idrico Integrato Sovrintendenza dei Beni Ambientali e del Paesaggio ATS Comunità Montane Enti Parco Vigili del Fuoco Gestori di servizi di rete TERNA

3.2 Soggetti interessati di cui vengono trattati i dati

Aspetto	Risposta/Descrizione
Qual è la **tipologia di soggetti interessati coinvolti?**	Legali rappresentanti o eventuali delegati (richiedente – gestore, referente IPPC o intermediario) Operatori (dipendenti/collaboratori dei soggetti giuridici che accedono alla piattaforma). Progettisti/professionisti per la redazione della documentazione necessaria Amministratori, i soci e familiari conviventi per i controlli antimafia Interessati che presentano osservazioni tramite apposito modulo ai sensi dell'art. 29 quater, comma 4, codice ambiente.
Fornire una stima del **numero di soggetti interessati coinvolti**	100-1000

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	**Per il legale rappresentante e/professionista, operatore delegato e interessati:** **Nome** **Cognome** **codice fiscale** **luogo e data di nascita** **residenza/domicilio** **indirizzo di posta elettronica certificata e non certificata** **recapito telefonico** **documento d'identità** **Solo per i professionisti: iscrizione all'ordine/albo/collegio**	**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** **I dati richiesti del legale rappresentante/ professionista/operatore sono necessari per presentare/integrare l'istanza e per i controlli previsti per legge.** **I dati dei professionisti relativi all'iscrizione all'albo consentono di accertarne qualifiche e responsabilità.** **I dati degli interessati a presentare osservazioni sono necessari per l'identificazione e eventuali interlocuzioni**

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		**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): dati dei progettisti e dei professionisti, dati dei conviventi, amministratori e soci per i controlli antimafia	**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**	Sì La raccolta e la consultazione è necessaria per l'avvio dell'istruttoria. La conservazione è necessaria le successive azioni correlate (controlli previsti dalla legge, mantenimento dei requisiti) 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	**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?**	**funzionari delle UO/Strutture competenti dell'istruttoria** **Sì, i funzionari sono profilati in BeS per l'istruttoria** **Team per il supporto di help desk e il supporto sistemistico (ARIA S.p.A.)** **Prefetture** **MASE** **Province** **Città Metropolitana di Milano** **Comuni** **ARPA Lombardia** **Autorità d'Ambito**

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
			Gestore del Servizio Idrico Integrato **Sovrintendenza dei Beni Ambientali e del Paesaggio** **ATS** **Comunità Montane** **Enti Parco** **Vigili del Fuoco** **Gestori di servizi di rete** **TERNA**

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 e i documenti raccolti sono conservati per 30 anni a decorrere dal rilascio dell’autorizzazione Sono fatti salvi, comunque, i tempi di conservazione dei dati personali previsti per l’ulteriore finalità di archiviazione dei documenti ai sensi di quanto indicato dalla normativa di riferimento e conformemente a quanto previsto dal «Aggiornamento Titolario di classificazione e Massimario di scarto dei documenti digitali ed analogici di Giunta Regionale» approvato con Decreto n. 4413 del 7 aprile 2026 e s.m.i. Indicare la tempistica prevista dal massimario di scarto: illimitato	per verificare la validità giuridico-amministrativa del procedimento durante il ciclo di vita dell’impianto; e per le verifiche e controlli successivi da parte di organi di audit, vigilanza o giurisdizionali.

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"

7.1 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 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	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?**	☒ 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	
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	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 ☐ In parte ☐ No ☐ N/A	……

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	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	.....
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	.....

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
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	

7.2 Piattaforma EDMA

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	Secondo gli standard di Aria S.p.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	Secondo gli standard di Aria S.p.A.
Access Management	**È previsto che le utenze abilitate ad accedere al sistema vengano create, modificate, riviste e cancellate**	☒ Si ☐ In parte ☐ No ☐ N/A	Per EDMA Regione Lombardia svolge una review dei propri utenti, richiedendo periodicamente l'estrazione degli utenti ad ARIA e svolgendo il controllo sulla base di una matrice RACI dei ruoli. Annualmente per gli utenti di RL è richiesta ad ARIA l'estrazione

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
			RACI dei profili. Per ARIA non è prevista una review periodica; è tuttavia in corso una revisione delle utenze
	È previsto che l'accesso al sistema avvenga attraverso una combinazione di username e password?	☐ Si ☒ In parte ☐ No ☐ N/A	Per EDMA l'accesso avviene normalmente da Intranet e richiede l'inserimento di userID e password valide. Recentemente è stata introdotta un'interfaccia che integra l'accesso attraverso regole IDPC-SPID (al momento la modalità IDPC e quella con user+password sono applicabili entrambe). E' attiva per ambedue le interfacce la possibilità di accedere in Single Sign On in quanto già autenticati al dominio di RL.
	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	Regole della password: • lunghezza (8 caratteri) • complessità (SI) • history (>10) • tentativi prima del lockout (NO) • scadenza (non oltre tre mesi dall'ultima password modificata) disabilitazione utenza dopo sei mesi di inattività dell'utenza. Suddividiamo due modalità: - password - IdPC
	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	L'applicativo è un gestionale interno e prevede l'autenticazione tramite credenziali valide e personali. Sono previsti i seguenti profili: • AdS, circa 15 persone, tra personale Aria, Engineering e BVTech; • Profili personalizzati in base agli uffici e ai ruoli operativi, che prevedono funzioni di inserimento documenti, firma e autorizzazione,

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
			mantenendo una certa segregazione dei ruoli operativi (tali profili sono associati a utenti SIREG (Regione Lombardia e ARIA)
	È previsto che per l'accesso ai sistemi venga richiesto un sistema di multi factor authentication?	☒ Si ☐ In parte ☐ No ☐ N/A	La nuova interfaccia applicativa prevede SPID livello 2 e la seconda modalità prevede l'accesso tramite VPN intranet.
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	Secondo gli standard di Aria S.p.A.
	È previsto che i file di log siano adeguatamente protetti da manomissioni e accessi non autorizzati?	☒ Si ☐ In parte ☐ No ☐ N/A	Secondo gli standard di Aria S.p.A.
	È previsto che le attività degli amministratori di sistema vengano registrate, analizzate e riviste periodicamente?	☒ Si ☐ In parte ☐ No ☐ N/A	Secondo gli standard di Aria S.p.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	Secondo gli standard di Aria S.p.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	è prevista la cifratura e l'accesso tramite 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	Sul nuovo modello applicativo vengono effettuate attività di VA/PT
	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	L'iter standard di rilascio delle patch di sicurezza, così come i rilasci applicativi, prevede la conduzione di attività di test in ambiente di integrazione tecnica.
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	Il backup standard previsto per la piattaforma EDMA è un backup full settimanale con retention di un mese e un backup incrementale ogni giorno con retention di una settimana. Il backup è svolto dal fornitore che ha in carico l'infrastruttura.
	È previsto che l'esecuzione del backup del sistema venga monitorato?	☒ Si ☐ In parte ☐ No ☐ N/A	Secondo gli standard ARIA
	È previsto vengano effettuati test periodici di Restore del Backup e test del Disaster Recovery?	☐ Si ☒ In parte ☐ No ☐ N/A	L'applicativo non prevede la verifica di Restore periodica ma rientra nel piano di disaster recovery.

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
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	Viene applicata la procedura standard di comunicazione dell'apertura, aggiornamento e chiusura dell'incident a tutti gli attori interessati.
	È previsto che in caso di Data Breach venga seguita la procedura di Data Breach definita dall'organizzazione?	☒ Si ☐ In parte ☐ No ☐ N/A	L'ufficio è al corrente delle procedure aziendali di gestione di incidenti e data breach qualora dovessero essere attivate.
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	I dipendenti sia di Regione Lombardia che di ARIA partecipano a corsi erogati sulle tematiche di privacy e sicurezza.
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:

L’informativa per la presentazione dell’istanza è presente in BeS con la funzione di flag bloccante per presa visione. Per gli interessati che presentano le osservazioni l’informativa è allegata al modulo messo a disposizione sull’apposita sezione del sito web regionale

☒ 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 Roberto Laffi in qualità di Direttore Generale della Direzione Ambiente e Clima 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.

Privacy Officer:

Dr. Gianluca Jesu

Per la Direzione: Ambiente e Clima

Dr. Roberto Laffi

Dirigente responsabile del procedimento Filippo Dadone

FILIPPO
DADONE
19.10.2026
08:41:57 UTC

PO competente per il procedimento Roberto Esposito

SPSRRT76A27F205T
/6030036279257005
.JQM4SG6OJLFLEW1K6UNTCEEYCMI=
ACTALIS S.P.A.
19.10.2026 07:57:26 UTC

Dirigente referente privacy Mariangela Criscione - Struttura Giuridico-Legislativo per l'ambiente

MARIANGELA
CRISCIONE
16.10.2026
10:11:20 UTC

PO referente privacy Elena Colao – EQ Referente giuridico privacy

CLOLGS64R55F205J/6030522188216000.SNCE0DWNWFOU3+DNA6KQJRO7IOY=
ACTALIS S.P.A.
15.10.2026 15:44:53 UTC

Referente Aria S.p.a; Silvia Osnago

SILVIA
OSNAGO
19.10.2026
11:14:15
GMT+01:00

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