Verbale

“Privacy By design e DPIA”

<Contributi regionali ***per l’accertamento degli usi civici***>

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

Revisione	Data	Sintesi delle Modifiche
	30/08/2023	Prima emissione

Indice

1 P1: “ANALISI DEL CONTESTO” 3
2 P2: “FINALITA’ E BASE GIURIDICA” 6
3 P3: “SOGGETTI COINVOLTI” 7
3.1 Soggetti che trattano i dati 7
3.2 Soggetti interessati di cui vengono trattati i dati 7
4 P4: “VALUTAZIONE DI NECESSITA’ E PROPORZIONALITA’” 9
4.1 Dati personali trattati 9
4.2 Operazioni sui dati 11
4.3 Accesso ai dati personali 13
5 P5: “DATA RETENTION” 15
6 P6: “DPIA: QUANDO E PERCHE’” 16
7 P7: “IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA” 18
EDMA 18
7 P7: “IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA” 24
BANDI ON LINE (BOL) 24
8 P8: “ADEMPIMENTI PRIVACY” 30

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

1 P1: “ANALISI DEL CONTESTO”

Aspetto	Risposta/Descrizione
Quali sono le **Direzioni di Regione Lombardia** coinvolte?	Direzione Generale Agricoltura, Sovranità alimentare e Foreste
Indicare il **nome dell’iniziativa/misura/servizio**	Assegnazione di contributi regionali alle Comunità Montane e ai Comuni che svolgono indagini funzionali all’accertamento degli usi civici.
Fornire una descrizione testuale **dell’iniziativa/misura/servizio.**	La L.R. 31/2008, all’articolo 165 comma 1 prevede che per le operazioni di accertamento degli usi civici, dove le stesse non siano state completate, Regione Lombardia e la Provincia di Sondrio, per il relativo territorio, si avvalgano delle indagini svolte dalle Comunità Montane o dai Comuni; stabilisce, inoltre, all’art.166 comma 1, che Regione Lombardia concede contributi a fondo perduto alle Comunità Montane o ai Comuni a tale scopo. Sono ammissibili le spese effettuate dai beneficiari relative ad incarichi a professionisti di comprovata esperienza, che non si trovino in situazioni di conflitto di interessi, per indagini documentali, in particolare per indagini di accertamento di usi civici. Sotto tale profilo, verranno trattati i dati relativi ai professionisti incaricati dai Comuni e dalle Comunità montane.
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., in qualità di responsabile, per la gestione delle piattaforme Bandi Online ed EDMA Comuni e Comunità montane che partecipano al bando avente ad oggetto l’erogazione di contributi per l’accertamento degli usi civici, in qualità di titolari autonomi, in forza della normativa di riferimento Provincia di Sondrio, in qualità di titolare autonomo

Indicare la **data** (anche approssimativa) di **avvio dell'iniziativa/misura/servizio**	04/09/2023
Quali sono le piattaforme informatiche che saranno utilizzate dal servizio informatico? (**esempi di piattaforme informatiche: EDMA, SIAGE, IDPC,**)	Bandi Online, EDMA
Il trattamento viene effettuato in modalità **cartacea** e/o con l'ausilio di **strumenti informatici**?	Modalità informatica
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:	

Il Bando prevede una prima fase in cui non vengono trattati i dati personali, in quanto la domanda di contributo viene presentata da Comuni e Comunità montane e viene erogato un anticipo agli enti stessi.

I dati personali dei professionisti, a cui vengono affidati gli incarichi da parte dei beneficiari del bando (Comuni e delle Comunità montane), vengono trattati da Regione Lombardia solo in fase di rendicontazione: i beneficiari li trasmettono alla Struttura "Sviluppo della montagna, foreste e tutela del suolo agricolo" di Regione Lombardia tramite la piattaforma Bandi Online, la quale genera una comunicazione cui è assegnato un numero di protocollo creato dal sistema informativo in uso in Regione Lombardia (EDMA).

La Struttura "Sviluppo della montagna, foreste e tutela del suolo agricolo", in sede di rendicontazione delle spese sostenute dai Comuni e dalle Comunità montane per l'accertamento degli usi civici, verifica la completezza e la correttezza formale della documentazione presentata in Bandi Online e tratta i seguenti dati personali dei professionisti incaricati: nome, cognome, codice fiscale, indirizzo, recapito telefonico, indirizzo mail, indirizzo pec, iban, curriculum vitae, inviando ai beneficiari eventuali comunicazioni/richieste di integrazione documentale anche tramite l'applicativo EDMA.

Per gli usi civici insistenti sulla Provincia di Sondrio, la Struttura della DG Agricoltura trasmette alla stessa, tramite EDMA, la relazione finale redatta dal professionista incaricato dai beneficiari del bando affinché possa adottare il decreto di accertamento degli usi civici sul territorio di propria competenza.

I dati personali sono conservati per 10 anni dall'erogazione dell'ultimo versamento o dalla decadenza/riduzione del contributo, per finalità di controllo e di gestione dell'eventuale contenzioso.

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: Erogazione di contributi regionali per l’accertamento degli usi civici **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.)** L.R. 31/2008 artt. 165 e 166 **Atti di normazione secondaria e delibere di giunta regionale** Deliberazione di giunta regionale n. XII/444 2023 del 12.6.2023 **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
Erogazione di contributi regionali per l’accertamento degli usi civici	Regione Lombardia	ARIA S.p.A., per le piattaforme EDMA e Bandi Online	Provincia di Sondrio, che riceverà la relazione tecnica preventiva per l’accertamento degli usi civici nel territorio di competenza. Comuni e Comunità montane che partecipano al bando per l’erogazione di contributi per l’accertamento degli usi civici

3.2 Soggetti interessati di cui vengono trattati i dati

Aspetto	Risposta/Descrizione
Qual è la **tipologia di soggetti interessati coinvolti?**	Professionisti esperti nell’ambito delle ricerche documentali che vengono incaricati dai Comuni o dalle Comunità montane.

Fornire una stima del **numero di soggetti interessati coinvolti**	0-200

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 (visure camerali) ☐Stato civile ☒Percorso professionale (CV) ☐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.(Iban) ☐Dati sulla posizione ☐Altro	I dati trattati sono comuni: dati anagrafici (cognome e nome, codice fiscale); di contatto (indirizzo, telefono, pec, indirizzo mail); identificativi di conti correnti (Iban) presenti nelle fatture rendicontate dai professionisti; percorso professionale dei professionisti incaricati (curriculum vitae)	**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 personali richiesti nel procedimento sono adeguati, pertinenti e limitati a quanto necessario per l’istruttoria della domanda e l’erogazione del contributo I dati sono trattati ai fini dell’acquisizione delle fatture e della documentazione relativa agli affidamenti degli incarichi ai professionisti per l’erogazione del contributo.

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 (Comuni e Comunità montane)	**Tutte le operazioni sui dati indicate sono necessarie per il raggiungimento della finalità del trattamento?** **Per ciascuna operazione giustificare per quale motivo viene svolta. Evitare operazioni non necessarie rispetto alle finalità.**	SI **La Raccolta** dei dati personali avviene quando i Comuni e le Comunità montane trasmettono alla Struttura "Sviluppo della montagna, foreste e tutela del suolo agricolo" la relazione finale redatta dal professionista incaricato e la rendicontazione delle spese relative agli incarichi. **La Consultazione** dei dati personali dei professionisti incaricati avviene nel corso della verifica sulla rendicontazione che Comuni e Comunità montane presentano a Regione Lombardia. La **Comunicazione** avviene nei confronti della Provincia di Sondrio, affinché la stessa possa adottare il decreto di accertamento degli usi civici sul territorio di propria competenza. **La Conservazione** dei dati personali avviene per 10 anni decorrenti dall'erogazione dell'ultimo versamento o dalla decadenza/riduzione del contributo, per finalità di controllo e di gestione dell'eventuale contenzioso.
	Vi è una pubblicazione o diffusione di dati personali? A quale scopo? Risulta applicabile/da applicare il principio di trasparenza?	NO
	È necessario realizzare copie dei dati personali (esempio: copie	NO

Indicare le operazioni sui dati	Domande utili per comprendere l'effettiva necessità e proporzionalità delle operazioni rispetto alle finalità	Risposta e giustificazione
	dell'archivio)? motivare la risposta	
	Le operazioni indicate includono l'impiego di algoritmi decisionali/trattamenti automatizzati che producono effetti giuridici sugli interessati?	NO
	Viene effettuata profilazione?	NO

4.3 Accesso ai dati personali

Indicare i soggetti preposti al trattamento dei dati e i relativi privilegi di accesso	Risposta e giustificazione	Domande utili per comprendere l'effettiva necessità e proporzionalità dell'accesso ai dati	Risposta e giustificazione
Quali sono i soggetti preposti al trattamento che accedono ai dati personali?	**Soggetti interni autorizzati** ☒Soggetti appartenenti alla DG ☒Soggetti della funzione sistemi informativi (operatori di EDMA e Bandi on Line) ☐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. (Provincia di Sondrio, Comuni, Comunità montane) ☐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.**	Soggetti appartenenti alla DG Agricoltura, in sede di rendicontazione ai fini dell'erogazione del contributo. Accedono ai dati gli Operatori di Bandi Online e EDMA per le attività connesse allo svolgimento del proprio lavoro. Dipendenti dei Comuni/Comunità Montane per l'affidamento dell'incarico ai professionisti e per la trasmissione a Regione Lombardia della rendicontazione. Dipendenti della Provincia di Sondrio, per l'eventuale successivo decreto di accertamento degli usi civici sul territorio di propria competenza.
		L'accesso è necessario/limitato rispetto alle attività che devono essere svolte?	SI
		Per ciascuna tipologia di utenti	SI

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
		sono stati stabiliti i privilegi di accesso?	
		I privilegi di accesso sono necessari/limitati rispetto alle attività che devono essere svolte?	SI

Eventuali note:

_____
_____
_____
_____

5 P5: “DATA RETENTION”

Tipologia dei dati trattati	Quantificare il tempo di conservazione dei dati.	C’è una legge che lo giustifica? Se si indicare quale Altrimenti fornire il criterio utilizzato per determinarlo
Dati dell’iniziativa/misura/servizio che stai considerando	Per la durata di 10 anni dall’erogazione dell’ultimo versamento o dalla decadenza/riduzione del contributo	Per finalità di controllo e di gestione di eventuale contenzioso

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”
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	……
	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	In preproduzione i dati sono necessari per effettuare i test e potrebbero essere in chiaro. In generale ci sono dati di utenze e comunque dati non sensibili

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	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 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	L'accesso all'applicativo 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).
	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

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	È previsto che i diritti di accesso al sistema, assegnati agli utenti, vengano rilasciati in base al principio della stretta pertinenza, del minimo privilegio e necessità per il ruolo di accedere e conoscere i dati (principio del need to know)?	☒ Si ☐ In parte ☐ No ☐ N/A	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, 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
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	Memorizzazione dei log applicativi all'interno del client sulla singola utenza. Viene inoltre fatto un monitoraggio esterno con lo strumento "Splunk", che consente di risalire ai servizi richiamati dal singolo utente.
	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	i log del server secondo procedure standard trasversali aziendali.

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
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	Sul client non è prevista la cifratura; la nuova interfaccia prevede la trasmissione via 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 saranno previste 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 LG che ha in carico l'infrastruttura.
	È previsto che l'esecuzione del backup del sistema venga monitorato?	☒ Si ☐ In parte ☐ No ☐ N/A	……

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	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.
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	E'stata condotta nel 2021 un'analisi dei rischi approfondita sulle componenti trasversali di EDMA, alla quale si aggiungeranno le verifiche privacy dedicate al trattamento in oggetto.
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	……

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

7 P7: “IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA”
BANDI ON LINE (BOL)

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

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

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

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	dall'ambiente di produzione?		
Access Management	**È previsto che le utenze abilitate ad accedere al sistema vengano create, modificate, riviste e cancellate,**	☒ Si ☐ In parte ☐ No ☐ N/A	……
	È previsto che l'accesso al sistema avvenga attraverso una combinazione di username e password?	☐ Si ☒ In parte ☐ No ☐ N/A	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	……

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
	È previsto che per l'accesso ai sistemi venga richiesto un sistema di multi factor authentication?	☒ Si ☐ In parte ☐ No ☐ N/A	……
Logging&Monitoring	**È prevista la generazione di file di log per tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione) con il dettaglio della data e dell'ora?**	☒ Si ☐ 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	E' previsto un rilascio nel corso del 2023 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/particolari direttamente nell'ambiente di

Area	Misura di sicurezza	Livello di implementazione	Note di commento e approfondimento
			progettazione di Bandi online e applicare una procedura di pseudonimizzazione tramite l'intervento del gestore del servizio
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	……

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

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

8 P8: “ADEMPIMENTI PRIVACY”

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

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

L’informativa privacy sarà allegata al bando e verrà veicolata dai Comuni e dalle Comunità montane partecipanti al bando ai professionisti interessati.

☒ 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:
_____
_____
_____
_____

Direttore Generale Agricoltura, sovranità alimentare e foreste Andrea Massari

Dirigente competente del procedimento Francesco Brignone

Dirigente referente privacy di Direzione Andrea Azzoni

PO competente per il procedimento Luisa Cagelli

PO referente privacy Elena Gomiero

Sistemi Informativi e ICT – PO delegata dal Dirigente per EDMA Andrea De Fre'

Sistemi Informativi e ICT – PO delegata dal Dirigente per "Bandi on Line" Silvia Eugenia Ronzio

ARIA S.p.A.: Service manager "Bandi on Line" Angelo Nitti

ARIA S.p.A.: Service manager EDMA: Cosmina Tufa

Privacy Officer Gianluca Jesu

La presente privacy by design viene formalizzata secondo quanto rappresentato dalla Direzione alla data del 30.08.2023