Allegato A

DESIGNAZIONE RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI IN OSSERVANZA ALL'ARTICOLO 28 DEL REGOLAMENTO UE 679/2016 ("RGDP")

CONTESTO DI RIFERIMENTO

LAZIOcrea S.p.A. (di seguito "LAZIOcrea" o "Società") è stata costituita con Legge Regionale n. 12 del 24 novembre 2014, a seguito di fusione per unione delle società Lazio Service S.p.A. e LAit S.p.A. (Lazio Innovazione Tecnologica).

I rapporti tra LAZIOcrea e la Regione Lazio sono regolati dalle disposizioni comunitarie, nazionali e regionali vigenti, dallo Statuto della Società, nonché dai contratti di servizio stipulati sulla base dei criteri e dei contenuti predefiniti con delibera della Giunta Regionale in conformità ai principi e alla normativa vigente.

LAZIOcrea è una società con capitale interamente regionale e opera nei confronti della Regione Lazio secondo le modalità dell'in house providing, nel rispetto delle direttive regionali in materia di esercizio del controllo analogo ed è soggetta ai poteri di programmazione, indirizzo strategico operativo e controllo della Regione, analogamente a quelli che quest'ultima esercita sui propri uffici e servizi, fatta salva l'autonomia della Società stessa nella gestione dell'attività imprenditoriale e nell'organizzazione dei mezzi necessari al perseguimento dei propri fini statutari.

LAZIOcrea, in relazione alle attività connesse all'esercizio di funzioni amministrative ex art. 118 della Costituzione per il perseguimento dei fini istituzionali regionali, espleta direttamente, in regime di "in house providing", per conto della Regione, oltre alle attività di progettazione, realizzazione e gestione del Sistema Informativo Regionale e del Data Center regionale, anche le funzioni di Organismo Intermedio e/o di Soggetto Attuatore di interventi co-finanziati dall'Unione Europea e di Centrale di Committenza.

L'art. 13 dello Statuto della LAZIOcrea, da ultimo approvato con Delibera della Giunta regionale n. 459 del 25/07/2017 (di seguito "DGR 459/2017") e con delibera dell'Assemblea straordinaria dei soci del 28/07/2017, prevede espressamente che i rapporti tra la Regione Lazio e LAZIOcrea siano regolati da uno o più contratti di servizi sulla base dei criteri e dei contenuti predefiniti dalla Giunta Regionale.

I rapporti tra la Regione Lazio e la società sono stati regolati con il contratto quadro relativo al periodo 2022-2026 approvato con DGR n. 952/2021, sottoscritto in data 29 dicembre 2021 e registrato al Registro cronologico n. 25960/2022 e sono declinati nel documento di programmazione denominato Piano Operativo Annuale (di seguito POA) approvato annualmente dalla Giunta Regionale; in data 29/12/2017 la Regione Lazio e LAZIOcrea hanno stipulato un Contratto Quadro di Servizi, entrato in vigore in data 1 Gennaio 2018 (Prot. LAZIOcrea n. 0306 del 10/01/2018), avente ad oggetto le attività affidate a LAZIOcrea a supporto dell'amministrazione regionale e degli enti alla stessa collegati.

I menzionati servizi svolti da LAZIOcrea per conto della Regione Lazio, così come pianificati attraverso la definizione del Piano Operativo Annuale (POA), comportano un trattamento di dati personali rientranti nella sfera di Titolarità dell'amministrazione stessa, ai sensi della normativa vigente in materia di protezione dei dati personali.

A tal proposito, la Regione Lazio, in qualità di Titolare del trattamento e in attuazione delle disposizioni vigenti in materia di protezione dei dati personali ha aggiornato i compiti e le responsabilità di Laziocrea, fornendo le istruzioni di cui all'art. 28 del Regolamento (DGR n. 797 del 29.11.2017, DGR n. 891 del 19 dicembre 2017 nel prosieguo rispettivamente "DGR 797/2017" e "DGR 891/2017");

Nell'allegato G alla suindicata DGR 797/2017 sono stati definiti analiticamente i compiti affidati a LAZIOcrea quale Responsabile del trattamento designato.

Con la Delibera della Giunta Regionale n. 840 del 20 dicembre 2018 (nel prosieguo DGR 840/2018) la Regione Lazio (Titolare del Trattamento) ha designato LAZIOCrea "Responsabile del trattamento" e, con Allegato G, ha ridefinito e/o aggiornato i compiti e le responsabilità attribuite alla LAZIOcrea con riferimento ai trattamenti dei dati personali effettuati per conto della Regione Lazio ai sensi dell'art. 28 del Regolamento (UE) 2016/679.

Con la Delibera della Giunta Regionale n. 952 del 16 dicembre 2021 (di seguito "DGR 952/2021") la Regione Lazio ha provveduto a modificare e aggiornare le precedenti DGR 840/2018 e DGR 797/2017 e ha definito il Contratto Quadro di Servizi relativo al periodo 2022-2026, nonché del Piano Operativo Annuale (di seguito POA) approvato annualmente dalla Giunta Regionale a norma dell'art. 3 del richiamato Contratto Quadro;– con le quali LAZIOcrea è stata designata "Responsabile del trattamento dei dati personali" – in osservanza dei vigenti parametri europei di cui all'art. 28 GDPR – sottoscritto in data 29 dicembre.

Con le Delibere della Giunta Regionale nn. 990 del 29 dicembre 2023, 1095 del 19 dicembre 2024 e 1324 del 30 dicembre 2025 la Regione Lazio ha provveduto rinnovare a LAZIOCrea la designazione a "Responsabile del trattamento dei dati personali" – in osservanza dei vigenti parametri europei relativi a compiti e istruzioni che il titolare assegna al responsabile secondo quanto previsto dall'art. 28 del Regolamento (UE) 2016/679.

CONTESTO NORMATIVO IN CUI OPERANO LE PARTI

In riferimento ai servizi affidati al fornitore con il "Contratto Principale" si specificano di seguito i ruoli privacy delle parti in riferimento alla normativa in materia di protezione dei dati personali.

- La Regione Lazio è Titolare del trattamento dei dati personali effettuato nell'ambito delle attività oggetto del sopra menzionato contratto principale.
- LAZIOcrea opera in qualità di Responsabile del trattamento dei dati personali rientranti nella sfera di titolarità della Regione Lazio con delega alla individuazione di sub-responsabili.
- Il Fornitore/Appaltatore, nell'ambito dei servizi affidati con contratto principale, opera in qualità di sub Responsabile del Trattamento dei suindicati dati personali di titolarità della Regione Lazio.
- LAZIOcrea è individuata come amministrazione sottoposta agli obblighi della legge 90/2024 ed alle indicazioni del Dlgs 138/2024 di recepimento della Direttiva 2555/2022 – Direttiva NIS2, di conseguenza, ciascun affidatario è sottoposto agli stessi obblighi per se e per la propria filiera di produzione compresi subappalti autorizzati.
- L'affidatario dovrà garantire che qualunque evento di sicurezza cibernetica sia comunicato a LAZIOcrea entro un massimo di 12 ore dalla verifica e dovrà dare tutto il supporto necessario per rispondere agli obblighi di legge e minimizzare l'impatto dell'evento.
- In osservanza all'art. 9 e art. 10 della legge 90/2024 l'affidatario (di qualunque tipo di compagine sociale), per se e per i propri sub-fornitori o sub-appaltatori, è obbligato a rispondere alle direttive sulla crittografia e sulle password rese disponibili dall'Agenzia per la Cybersicurezza Nazionale e dal Garante per la Protezione dei Dati Personali, e/o dal Centro Nazionale di Crittografia nella versione valida al momento di consegna del prodotto.
- L'affidatario, e la propria filiera produttiva di cui si rende garante, in caso di sviluppo e/o manutenzione di software applicativo, è obbligato a seguire le linee guida sullo sviluppo sicuro rese disponibili da ACN e AgID come eventualmente dettagliato in apposito allegato.

TUTTO CIO' PREMESSO

il Responsabile del trattamento, alla sottoscrizione del presente Contratto, attenendosi alle istruzioni impartite dal Titolare nel pieno rispetto di quanto imposto dall'art. 28, par. 3, si impegna a mettere in atto misure tecniche e organizzative adeguate in modo tale che i trattamenti soddisfino i requisiti del GDPR e garantiscano la tutela dei diritti e delle libertà degli interessati.

Le parti stipulano e convengono quanto segue:

SEZIONE I

1. Clausola 1

Scopo e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
b) I titolari del trattamento e i responsabili del trattamento, di cui all'allegato I, hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.
c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.
d) Gli allegati da I a IV costituiscono parte integrante delle clausole.
e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.
f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

2. Clausola 2

Invariabilità delle clausole

a) Le parti si impegnano a non modificare le clausole come qui esposte se non per aggiungere o aggiornare informazioni negli allegati.
b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

3. Clausola 3

Interpretazione

3.1. Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679 o nel regolamento (UE) 2018/1725, tali termini hanno lo stesso significato di cui al regolamento interessato.
b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.
c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

4. Clausola 4

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

5. Clausola 5

Clausola di adesione successiva

a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di Titolare del trattamento o di Responsabile del trattamento, compilando gli allegati e firmando l'allegato I.
b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un Titolare del trattamento o di un Responsabile del trattamento, conformemente alla sua designazione nell'allegato I.
c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II

OBBLIGHI DELLE PARTI

6. Clausola 6

Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

7. Clausola 7

Obblighi delle parti

7.1. Istruzioni

a) Il *responsabile* del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il *responsabile* del trattamento. In tal caso, il *responsabile* del trattamento informa il *titolare* del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il *titolare* del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.
b) Il *responsabile* del trattamento informa immediatamente il *titolare* del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il *responsabile* del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del *titolare* del trattamento.

7.3. Durata del trattamento dei dati personali

Il *responsabile* del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II. Al termine del trattamento il *responsabile* emette comunicazione formale verso il *titolare* in cui informa che da quel momento tutti i trattamenti dell'accordo sono interrotti.

7.4. Sicurezza del trattamento

a) Il *responsabile* del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.
b) Il *responsabile* del trattamento concede l'accesso ai dati personali, oggetto di trattamento, ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il *responsabile* del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili – Dati particolari

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il *responsabile* del trattamento applica limitazioni specifiche e/o garanzie supplementari. Tali garanzie supplementari sono esplicitate nell'allegato III.

7.6. Documentazione e rispetto

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.
b) Il *responsabile* del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del *titolare* del trattamento relative al trattamento dei dati conformemente alle presenti clausole.
c) Il *responsabile* del trattamento mette a disposizione del *titolare* del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679. Su richiesta del *titolare* del trattamento, il *responsabile* del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il *titolare* del trattamento può tenere conto delle pertinenti certificazioni in possesso del *responsabile* del trattamento.
d) Il *titolare* del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del *responsabile* del trattamento e, se del caso, sono effettuate con un preavviso ragionevole, non inferiore a 2 settimane. *Resta inteso che il Titolare o il Responsabile avranno la facoltà di incaricare dei professionisti indipendenti per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report ("Report"). Tali Report, che costituiscono informazioni confidenziali, potranno essere resi disponibili al SubResponsabile per consentirgli di verificare le eventuali azioni correttive da implementare in funzione al presente Accordo. Il Titolare o Responsabile dovranno previamente inviare richiesta scritta di Audit all'indirizzo del SubResponsabile. Successivamente alla richiesta di audit o ispezione il SubResponsabile e il Titolare o Responsabile concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche (raccomandando l'utilizzo degli standard ISO 19011). Il titolare (Regione LAZIO) e il Responsabile (LAZIOcrea) sono di principio vincolati alla riservatezza e comunicheranno al sub-responsabile i soggetti che compongono il gruppo di Audit*

(auditor/revisori) e si impegnano a far sottoscrivere eventuali accordi di riservatezza specifici in caso gli auditor non siano dipendenti o collaboratori del Titolare e/o del Responsabile. Il SubResponsabile potrà opporsi per iscritto alla nomina da parte del Titolare o Responsabile di eventuali auditor/revisori esterni se questi possano rappresentare soggetti concorrenti del SubResponsabile. In tali circostanze il Titolare o il Responsabile saranno tenuti a nominare altri auditor/revisori o a condurre le verifiche in proprio. Restano a carico esclusivo del Titolare o del Responsabile i costi delle attività di verifica dallo stesso commissionate a eventuali terzi.

e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a ulteriori sub-responsabili del trattamento

a) Il *responsabile* del trattamento ha l'autorizzazione generale del *titolare* del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il *responsabile* del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 20 giorni, dando così al *Titolare* del trattamento tempo sufficiente per potersi opporre. Il Responsabile del trattamento fornisce al *Titolare* del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b) Qualora il *responsabile* del trattamento ricorra a un *sub-responsabile* del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del *responsabile* del trattamento), stipula un contratto che impone al *sub-responsabile* del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al *responsabile* del trattamento conformemente alle presenti clausole. Il *responsabile* del trattamento, ove possibile, si assicura che il *sub-responsabile* del trattamento rispetti gli obblighi cui il *responsabile* del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679.

c) Su richiesta motivata del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

e) Il *responsabile* del trattamento concorda con il *sub-responsabile* del trattamento una clausola del terzo beneficiario secondo la quale, qualora il *sub-responsabile* del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il responsabile o il titolare del trattamento hanno diritto di risolvere il contratto con il *sub-responsabile* del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

f) Il Subresponsabile (appaltatore) mantiene un elenco completo di tutti gli ulteriori responsabili (sub-sub-responsabili autorizzati) con indicazione di ragione sociale e persone chiave di riferimento contattabili. L'elenco deve essere consegnato a richiesta entro un massimo di 8 ore dalla richiesta senza necessità di motivazione. Rimane responsabilità dell'appaltatore informare tutti i sub-sub responsabili delle eventuali possibili richieste di informazioni che potranno essere effettuare dal committente e/o dal titolare ed eventualmente rispondere alle richieste in loro vece assumendo su di se tutti i rischi.

7.8. Trasferimenti internazionali

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del *responsabile* del trattamento è effettuato soltanto su istruzione documentata del *titolare* del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.

b) Il *titolare* del trattamento conviene che, qualora il *responsabile* del trattamento ricorra a un *sub-responsabile* del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del *titolare* del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il *responsabile* del trattamento e il *sub-responsabile* del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

h) Clausola 8

Assistenza al titolare del trattamento

a) Il *responsabile* del trattamento notifica prontamente al *titolare* del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal *titolare* del trattamento.

b) Il *responsabile* del trattamento assiste il titolare nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il *responsabile* del trattamento si attiene alle istruzioni del *titolare* del trattamento.

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il *responsabile* del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del *responsabile* del trattamento:

   i) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

   ii) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

   iii) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il *titolare* del trattamento qualora il *responsabile* del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

   iv) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il *responsabile* del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

i) Clausola 9

Notifica di un incidente di sicurezza – soggetto nel perimetro della Legge 90/2024 e Dlgs 138/2024.

In caso di un incidente di sicurezza come qualificato dalla Legge 90/2024 e/o dal D.lgs. 138/2024 (recepimento Direttiva 2022/2555 – NIS2), il *responsabile* del trattamento comunica a LAZIOcrea entro un massimo di 12 ore l'evento accaduto a uno qualunque dei soggetti coinvolti nel progetto e si rende disponibile a coopera con il titolare e/o con il responsabile del trattamento ed eroga assistenza nell'adempimento degli obblighi che incombono sul Titolare e sul responsabile. Tali attività di assistenza effettuate a seguito di un incidente non costituiscono a generare costi per LAZIOcrea. Le modalità di gestione dei rapporti fra sub-responsabile e responsabile possono essere le stesse riportare ai sotto riportati punti 9.1 e 9.2 dove tutti gli

obblighi si intendono riferiti alla Legge 90/2024 e Dlgs 138/2024.

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il *responsabile* del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679 tenuto conto della natura del trattamento e delle informazioni a disposizione del *responsabile* del trattamento.

9.1 Violazione riguardante dati trattati dal titolare e/o dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il *responsabile* del trattamento, assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679 devono essere indicate nella notifica del titolare del trattamento e includere almeno:
   i) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   ii) le probabili conseguenze della violazione dei dati personali;
   iii) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal sub-responsabile del trattamento

In caso di una violazione dei dati personali trattati dal *responsabile* del trattamento, quest'ultimo ne dà notifica al *titolare* del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
Le parti stabiliscono nell'allegato III tutti gli altri elementi che il *responsabile* del trattamento è tenuto a fornire

quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III

DISPOSIZIONI FINALI

j) Clausola 10

Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il *responsabile* del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il *titolare* del trattamento può dare istruzione al *responsabile* del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il *responsabile* del trattamento informa prontamente il *titolare* del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Il *titolare* del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:
   i) il trattamento dei dati personali da parte del *responsabile* del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
   ii) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;
   iii) il *responsabile* del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679;

c) Il *responsabile* del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il *titolare* del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il *titolare* del trattamento insista sul rispetto delle istruzioni.

d) Dopo la risoluzione del contratto il *responsabile* del trattamento restituisce al *titolare* del trattamento tutti i dati personali e cancella le copie esistenti in suo possesso certificando al responsabile di averlo fatto, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il *sub-responsabile* del trattamento continua ad assicurare il rispetto delle presenti clausole.

ALLEGATO I

Elenco delle parti

Titolare/i del trattamento:
Nome: REGIONE LAZIO
Direzione: CULTURA, POLITICHE GIOVANILI E DELLA FAMIGLIA, PARI OPPORTUNITA', SERVIZIO CIVILE

Responsabile/i del trattamento
LAZIOcrea S.p.a.
Sede legale: Via Anagnina 203
001118 – ROMA (RM)
Tel. (+39) 06 51681600
PEC: laziocrea@legalmail.it

Nome, qualifica e dati di contatto del referente:
(opzionale -Inserire nome referente interno)

Firma e data di adesione: .....
(Delegato Privacy [1]LAZIOcrea s.p.a.)

SubResponsabile del trattamento
Inserire i dati per fornitore. In caso di RTI sarà compito del mandatario coordinarsi perché gli stessi patti e condizioni siano definiti con ogni singolo mandante, definendo in modo preciso le differenti responsabilità sul trattamento. Il mandatario firma questa DPA per tutti i mandanti come previsto dalle regole sugli appalti e sulla composizione delle RTI.

Firma e data di adesione: .....
(firmatario del contratto)

.....

[1] Soggetto che firma il contratto

ALLEGATO II

Descrizione del trattamento

Il sub Responsabile del trattamento fornisce il Software SEBINA (installato su CED regionale) e attività ivi connesse di manutenzione adeguativa e correttiva per la gestione dei servizi bibliotecari a favore delle biblioteche che afferiscono al Polo bibliotecario Regionale RL1. Pertanto il trattamento del sub responsabile consiste nella gestione e manutenzione del SW.

Il SW SEBINA (di seguito Piattaforma) effettua raccolta, gestione e archiviazione dei dati personali degli utenti delle Piattaforma stessa. Gli utenti della Piattaforma sono: i cittadini che si registrano con username e password (credeziali SPEAD) o iscritti alle biblioteche per effettuare ricerche e/o richieste di materiale didattico; gli operatori delle Biblioteche per effettuare i servizi di catalogazione e gestione delle richieste dei cittadini (utenti registrati della piattaforma o clienti delle biblioteche); gli operatori della Direzione Regionale competente per le attività di monitoraggio e gestione del Polo bibliotecario nonché (in qualità di AdS) per la creazione delle credenziali di accesso alla Piattaforma degli operatori delle Biblioteche afferenti al POLO; Gli AdS del Fornitore della Piattaforma .

Di seguito si riportano le funzionalità della piattaforma Sebina:

- *componenti di back-office (ad uso degli operatori delle biblioteche, dei gestori delle biblioteche e degli Amministratori del sistema bibliotecario) per la gestione delle attività svolte dalle biblioteche: prestiti, utenti, digital reference, catalogo, acquisti, periodici, report e statistiche, generazione di open data, …*
- *componenti di front-office (ad uso degli utenti), per la consultazione e fruizione online del catalogo e dei servizi, in modalità web e sui dispositivi mobile, attraverso le App native o tramite apparecchiature di Autoprestito (di fornitori terzi) in colloquio con Sebina.*

Per ulteriori dettagli, si rimanda alla DPIA condotta nel mese di gennaio 2025.

Categorie di interessati i cui dati personali sono trattati

Cittadini che usufruiscono dei servizi bibliotecari (Utenti/registrati della Piattaforma o iscritti delle biblioteche); persone fisiche/legali rappresentanti dei Fornitori di materiale didattico delle biblioteche iscritte al Polo; operatori della Biblioteche; AdS o utenti della Regione Lazio per le attività di gestione del Polo bibliotecario; AdS Fornitore Piattaforma

Categorie di dati personali trattati
Per ciascuna categoria di interessati segnalare quali categorie di dati personali sono raccolti.
Ricordare sempre di inserire: i dati di tracciamento se raccolti anche attraverso cookie o altri; i dati delle utenze di accesso ai sistemi, i dati degli amministratori di sistema.
Sarà compito delle informative definire tutti i trattamenti che verranno effettuati attraverso l'esercizio sugli ambienti operativi di LAZIOcrea – Regione LAZIO.
Ricordarsi di evidenziare le categorie di dati particolari per i quali vanno inserite le eccezioni previste dall'art. 9 del GDPR e dell'art. 10 del GDPR.

Non rileva la qualifica dell'interessato (ad es, imprenditore, amministratore, detenuto, etc): il trattamento in esame si rivolge a tutti gli utenti e fornitori delle Biblioteche del Polo bibliotecario e, per questi, vengono raccolti i seguenti dati: I dati identificativi e di contatto degli "utenti" iscritti presso una biblioteca aderente al Polo, inseriti nell'anagrafica utenti condivisa del Polo SBN RL1 (nome e cognome, data e luogo di nascita,

codice fiscale, sesso, nazionalità, estremi del documento di identità, indirizzo di residenza, telefono e mail da utilizzare per comunicazioni relative ai servizi richiesti, categoria professionale di appartenenza), eventualmente confluiti attraverso SPID (o TS-CNS,CIE). Al fine di garantire la funzionalità del servizio di prestito, inclusi il prestito interbibliotecario e quello intersistemico, erogato dalle biblioteche aderenti al Polo, confluiscono nell'anagrafica utenti del Polo anche i dati inerenti ai prestiti di materiale documentale in corso di fruizione da parte degli utenti iscritti, i quali sono disponibili per il trattamento esclusivamente da parte delle biblioteche in cui l'utente è iscritto o associato.
I dati identificativi e di contatto dei "fornitori" del materiale librario e documentario acquisito dalle biblioteche del Polo inseriti nell'anagrafica fornitori del Polo SBN RL1 al fine di costituire un albo fornitori comune (nome e cognome, indirizzo, contatti di recapito ed altri dati necessari alla identificazione e al contatto del fornitore) nonché i dati relativi alle condizioni applicate e ai servizi e forniture offerte a tutte le biblioteche del Polo (con esclusione dei dati specifici relativi al rapporto tra singolo cliente e fornitore, come ad es. condizioni commerciali offerte a una singola biblioteca e non all'intero Polo, protocolli speciali di ordine e fatturazione, singoli ordini e fatture ecc., per i quali i trattamenti restano quindi riservati alla singola biblioteca che effettua l'ordine).
Inoltre i dati comuni di log degli utenti e degli amministratori (autorizzati al trattamento) e anche i dati dei componenti del gruppo di progetto interni ed esterni.

Categorie di interessati	***Categorie di Dati Personali***	***Annotazioni***
☒ Utenti navigatori di siti web	☒ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☒ D7 Dati utenze ☒ D8 Dati tracciamento informatico	*Dati degli utenti della Piattaforma (cittadini che usufruiscono del servizio che gli operatori delle biblioteche e della Regione Lazio)* *Ivi compresi dati di tracciamento informatico, di log* *Per D7 si considerano comprese anche credenziali spid*
☐ Amministratori di Società	☐ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☐ D8 Dati tracciamento informatico	
☐ Imprenditori	☐ D1 Dati anagrafici	

	☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☐ D8 Dati tracciamento informatico	
☐ Beneficiari di finanziamenti	☐ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☐ D8 Dati tracciamento informatico	
☐ Dipendenti e familiari	☐ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☐ D8 Dati tracciamento informatico	
☒ Amministratori di Sistema	☒ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☒ D7 Dati utenze	*log di accesso al sistema e credenziali di accesso come indicate sopra*

	☒ D8 Dati tracciamento informatico	
☐ Personale di imprese comprese ASL e similari	☐ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☐ D8 Dati tracciamento informatico	
☒ Visitatori di siti e/o plessi	☐ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☒ D8 Dati tracciamento informatico	*Cittadini che consultano la piattaforma senza registrarsi*
☒ Cittadini	☒ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☒ D8 Dati tracciamento informatico	*Utenti della Piattaforma (vedi sopra)* *iscritti alle biblioteche che usufruiscono del servizio e dunque insereriti a sistema.* *Informazioni relative alle richieste di prestito e/o servizio in corso*
☐ Assistiti del servizio sanitario	☒ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari	

	☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☐ D8 Dati tracciamento informatico	
☐ Minori	☒ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☐ D8 Dati tracciamento informatico	
☐ Detenuti	☐ D1 Dati anagrafici ☐ D2 Dati relativi a titoli di studio, licenze e altre certificazioni professionali ☐ D3 Dati retributivi ☐ D4 Dati bancari ☐ D5 Dati appartenenti a categorie particolari ☐ D6 Dati giudiziari ☐ D7 Dati utenze ☐ D8 Dati tracciamento informatico	
(Altri indicare)		

Natura del trattamento

Raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione anche a fini statistici, consultazione, uso, diffusione o qualsiasi altra forma di messa a disposizione ad organi istituzionali esterni, raffronto o interconnessione, limitazione, cancellazione o distruzione.

Per il tramite del proprio responsabile e subresponsabile del trattamento, effettua i trattamenti necessari a garantire la funzionalità della piattaforma informatica per la gestione del Polo, in particolare quelli volti alla organizzazione, strutturazione, conservazione, blocco e distruzione dei dati presenti nell'anagrafica utenti e nell'anagrafica fornitori della piattaforma informatica del Polo. Per il tramite degli operatori autorizzati/incaricati della propria Biblioteca giuridica e dei beni culturali "Altiero Spinelli" effettua la consultazione, utilizzo e aggiornamento dei dati personali degli utenti presenti nell'anagrafica utenti della piattaforma informatica del Polo; la raccolta e registrazione dei dati personali dei propri utenti e registrazione e modifica dei dati relativi ai prestiti documentali effettuati dai propri utenti (cioè quelli iscritti o associati

alla biblioteca); la raccolta, registrazione, modifica, selezione, consultazione, utilizzo e cancellazione dei dati personali inerenti ai fornitori presenti nell'anagrafica fornitori della piattaforma informatica del Polo.

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

Finalità condivise tra Regione Lazio e biblioteche iscritte al Polo:
- sviluppo, sostegno, integrazione e interconnessione delle biblioteche presenti sul territorio regionale e del relativo servizio di lettura offerto al pubblico (inclusi i servizi di consultazione, prenotazione, prestito, anche interbibliotecario e intersistemico, e document delivery);
- salvaguardia e diffusione dei patrimoni documentali detenuti, anche mediante la circolazione dei materiali e l'adeguamento di tutte le biblioteche aderenti, sia pubbliche che private, agli standard definiti per la catalogazione e la fornitura dei servizi;
- sviluppo della cooperazione per la formazione e l'incremento del catalogo collettivo e della rete del S.B.N. (Sistema Bibliotecario Nazionale);
- implementazione di nuovi modelli di fruizione del patrimonio documentario mediante strumenti digitali e telematici (incluso il prestito o la consultazione di risorse digitali);
- creazione di legami stabili di tipo collaborativo, anche mediante piattaforme e archivi digitali condivisi, tra i soggetti coinvolti nell'erogazione del servizio pubblico di lettura;
- realizzazione di analisi e valutazioni inerenti alla funzionalità e alle necessità del S.B.N.;
- realizzazione di analisi statistiche anche finalizzate alla raccolta e trasmissione all'ISTAT ai fini del rispetto delle disposizioni vigenti in materia di sistema statistico nazionale ai sensi dell'art. 7 del d.lgs. n. 322/1989, del Programma statistico nazionale e dei relativi aggiornamenti annuali adottati con DPR.

Basi giuridiche: esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui le Parti sono investite in relazione alla erogazione del servizio pubblico di lettura e alla conservazione, fruizione e valorizzazione del patrimonio culturale di cui dispongono (art. 6, comma 1 lett. e) del GDPR.

Finalità per le quali il sub Responsabile (Fornitore) tratta i dati sopra indicati è la regolare esecuzione delle attività oggetto di contratto/Affidamento. Base giuridica art 6 lett b) GDPR (esecuzione di un contratto)

Durata del trattamento

Finché i dati non sono restituiti e cancellati in modo sicuro con comunicazione al responsabile, il SubResponsabile del trattamento continua ad assicurare il rispetto di questo accordo in tutte le sue parti.
Occorre specificare la durata del trattamento collegata a questo accordo e non la durata del trattamento effettuata dal titolare. Ricordarsi di inserire una clausola tipo:

- *Durata del contratto maggiorata di 6 mesi con obbligo del responsabile di comunicare l'interruzione dei trattamenti e la cancellazione dei dati in suo possesso con atto formale. Fermo restando ulteriori proroghe alle prestazioni contrattuali (31.12.2025 è la scadenza attualmente prevista).*

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

- *Eventuali sub-subresponsabili devono rispettare le stesse misure di sicurezza applicate al primo responsabile.*

ALLEGATO III – RICHIESTE AL FORNITORE SUBRESPONSABILE

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati

Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.
Le misure di sicurezza qui citate sono da applicare al gruppo di progetto (compresi gli eventuali subaffidatari) e al prodotto.
Le misure di sicurezza del trattamento sono da scegliere fra quelle riportate su (scegliere gli annessi compresi ricordando che ANNESSO 2 e ANNESSO 3 sono alternativi fra loro e spesso non necessitano di altri ANNESSI):

- ☐ *ANNESSO 1 – Misure di sicurezza da applicare per lo sviluppo di applicazioni (gestionali);*
- ☒ *ANNESSO 2 – Misure di sicurezza da applicare per sistemi gestiti dall'appaltatore presso il data center locale;*
- ☐ *ANNESSO 3 – Misure di sicurezza da applicare per sistemi gestiti dall'appaltatore presso un data center sotto il controllo dell'appaltatore.*
- ☒ *ANNESSO 4 – Altre misure di sicurezza (adottabili in aggiunta a quanto definito in ANNESSO 1).*

La scelta degli allegati da rispettare deve essere fatta dal committente (gestore del contratto). Tutti gli sviluppi software sono da considerare come "software gestionali" a meno che non si rientri in particolari ambiti applicativi più restrittivi o governati da specifiche legislazioni che l'appaltatore è tenuto a conoscere. Gli allegati sono ripresi dal "CODICE DI CONDOTTA PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO DALLE IMPRESE DI SVILUPPO E PRODUZIONE DI SOFTWARE GESTIONALE - (Pubblicato sulla Gazzetta Ufficiale Serie Generale del 278 del 27/11/2024) - PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI N. 618 DEL 17/10/2024"
L'affidatario può fare riferimento alla adesione (dimostrabile) ad un codice di condotta per ridurre le clausole di sicurezza previste dagli ANNESSI.

In ogni caso il prodotto software deve sempre rispettare le misure generali previste dalla Legge 90/2024, dal Dlgs 138/2024 (recepimento della Direttiva NIS 2), dalle linee guida sullo sviluppo sicuro emanata da AgID e/o da ACN, dalle linee guida sull gestione delle password e della crittografia emanate da ACN.
Il prodotto deve essere certificabile ai sensi della normativa specifica dell'ambito del prodotto sviluppato (ad esempio presidi medici o similari), e deve essere certificabile ai sensi della protezione dei diritti e libertà degli interessati come indicato dell'art. 42 GDPR.

LAZIOcrea è società certificata ISO 27001, ISO27017, ISO27018 e applica i controlli previsti alla filiera produttiva.
In caso di sviluppo e/o manutenzione di applicazioni software il gruppo di progetto è obbligato a presentare documenti che attestino i requisiti delle tabelle 9, 10 e 11 allegate al documento "Linee guida - La sicurezza nel procurement ICT" pubblicate da AgID nel Aprile 2020 ed eventualmente aggiornate. (https://trasparenza.agid.gov.it/page/9/details/1641/determinazione-n-2202020-del-17-maggio-2020-adozione-delle-linee-guida-la-sicurezza-nel-procurement-ict.html) che qui si riportano in estratto:

TABELLA 9: REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI SVILUPPO APPLICATIVO

R20	Il fornitore deve attenersi alla politica di sicurezza dell'amministrazione committente, con particolare riferimento all'accesso ai dati dell'amministrazione, che avverrà esclusivamente sui sistemi di sviluppo e test.
R21	In fase di analisi, il fornitore deve definire le specifiche di sicurezza (non funzionali) a partire dai requisiti espressi dall'amministrazione.
R22	In fase di progettazione codifica, il fornitore deve implementare le specifiche di sicurezza nel codice e nella struttura della basedati.
R23	Al termine del progetto, il fornitore deve rilasciare tutta la documentazione necessaria all'amministrazione per gestire correttamente quanto rilasciato anche sotto l'aspetto della sicurezza.

TABELLA 10: REQUISITI SPECIFICI PER FORNITURE DI OGGETTI CONNESSI IN RETE

R24	Supporto di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.).
R25	Filtraggio di indirizzi IP.
R26	Supporto di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.).
R27	Gestione di più profili con privilegi diversi.
R28	Funzionalità di "richiesta creazione o cambio della password al primo accesso".
R29	Blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso.
R30	Gli accessi degli utenti devono essere registrati su un archivio (log) non cancellabile con il reset.
R31	Gestione dei log di sistema (accessi, allarmi, ecc.).
R32	Il fornitore (anche in collaborazione con il produttore della tecnologia) deve offrire processi, unità organizzative e strumenti dedicati alla gestione di vulnerabilità scoperte sui prodotti oggetto della fornitura.
R33	Per gli apparati proposti deve essere disponibile documentazione tecnica (schede tecniche, manuali, guide operative) relativa alla corretta configurazione e gestione degli aspetti di sicurezza.

TABELLA 11: REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI GESTIONE REMOTA

R34	I meccanismi di autenticazione devono essere basati su meccanismi di crittografia asimmetrica, a chiave pubblica; la lunghezza delle chiavi va impostata sulla base della criticità della comunicazione da cifrare (ad esempio 256 bit per le meno critiche, 512 bit per le più critiche). La gestione e distribuzione delle chiavi e dei certificati è a carico del fornitore.
R35	Autorizzazione: sulla base delle credenziali fornite dall'utente, si devono individuare i diritti e le autorizzazioni che l'utente possiede e permetterne l'accesso alle risorse limitatamente a tali autorizzazioni.
R36	Confidenzialità nella trasmissione dei dati: le comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'amministrazione devono essere cifrate.
R37	Fornire meccanismi che permettano di garantire l'integrità di quanto trasmesso (ad esempio meccanismi di hashing).
R38	Il fornitore deve descrivere nel dettaglio le soluzioni tecniche utilizzate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza, ...) per soddisfare i requisiti di sicurezza dell'amministrazione committente.
R39	In fase di attivazione del servizio, il fornitore deve concordare con l'amministrazione le modalità operative e le politiche di sicurezza, i livelli di gravità degli incidenti, le attività e le contromisure che dovranno essere svolte per contrastare le minacce.
R40	Il fornitore dovrà attenersi alle politiche di sicurezza definite dalla committente, con particolare riferimento alla definizione di ruoli e utenze per l'accesso ai sistemi gestiti.
R41	In caso di necessità, da parte degli operatori, di accesso a Internet, il fornitore deve utilizzare un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dall'amministrazione.
R42	In caso di rilevazione di un incidente di gravità elevata (con scala da definire a inizio fornitura), il fornitore deve dare immediata notifica, tramite canali concordati con l'amministrazione, dell'incidente rilevato e delle azioni da intraprendere, al Responsabile della Sicurezza indicato dall'amministrazione e agli organismi individuati dal legislatore a presidio della sicurezza cibernetica.
R43	Per ogni incidente di sicurezza, il fornitore s'impegna a consegnare all'amministrazione, entro il giorno successivo, un report che descriva la tipologia di attacco subito, le vulnerabilità sfruttate, la sequenza temporale degli eventi e le contromisure adottate.
R44	Su richiesta dell'amministrazione, il fornitore deve consegnare i log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT. Tali log dovranno essere inviati all'amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta.
R45	Il fornitore deve monitorare la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite. Entro il giorno successivo al rilascio dell'upgrade/patch/hotfix, il fornitore deve avviare una valutazione, da rilasciarsi entro un numero giorni da stabilirsi, propedeutica all'installazione delle stesse sui dispositivi di sicurezza, che ad esempio identifichi la possibilità di applicare la patch immediatamente, o la necessità di apportare MEV o integrazioni prima di procedere alle installazioni.

ANNESSO 1 – Misure di sicurezza da applicare per lo sviluppo di applicazioni (gestionali)

Ambito (Da Allegato A – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato A – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato A – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato A – Codice Condotta SW Gestionali)**	**RID**
Principi di sviluppo del SW Gestionale	Analisi di nuove funzioni	Valutazione e documentazione nelle analisi delle funzioni applicative del rispetto dei principi di minimizzazione: - nel dato: ogni dato personale raccolto dal SW deve essere necessario rispetto alla finalità della raccolta - nell'uso: ogni dato personale deve essere trattato solo da coloro che ne abbiano un'effettiva necessità - nel tempo: il dato personale deve essere trattato per il tempo strettamente necessario per il perseguimento della finalità. In particolare, già in fase di analisi devono essere identificati i dati personali trattati, la durata prevista dal trattamento, l'indicazione dei ruoli che vi potranno accedere, l'indicazione dei processi che vi potranno accedere, l'indicazione degli output.	ISO/IEC 27701:2019 A.7.4.4	RID
Definizione della protezione dell'accesso ai dati	Documentazione degli strumenti e dei requisiti per l'utilizzo del SW	Documentazione degli strumenti utilizzati per trattare i dati (indicazione del DB utilizzato, strumento di scrittura del codice, sistema di conservazione dei documenti prodotti), definendo le misure di sicurezza poste a tutela dei dati (profili di accesso al DB, crittografia del DB, dialogo tra applicazione e DB e protezione delle password, ecc.). Documentazione dei sistemi operativi e dei requisiti per l'utilizzo del SW.	ISO/IEC 27701:2019 A.7.4.2, A.7.4.4	
Autenticazione	Modalità e regole di autenticazione	Utilizzo di utenze nominative individuali al fine di garantire la tracciabilità delle operazioni eseguite. Conformità della password policy alle best-practice europee e internazionali di riferimento che ne garantiscano sicurezza adeguata, sia in termini di complessità (es. minimo 8 caratteri presenza di caratteri speciali, maiuscole, etc.), scadenza (durata fissa o modulabile dal cliente/titolare del trattamento), ciclicità della password (es. non consentire il riuso di password precedenti), gestione reset delle password con sistemi che garantiscano l'identificazione del richiedente e simili. Adozione di misure per prevenire e contrastare attacchi informatici di tipo credential stuffing (testing username/password pairs obtained from the breach of another site), brute force (testing multiple passwords from dictionary or other source against a single account) e password spraying (testing a single weak password against a large number of different accounts).	ISO/IEC 27002:2022 5.15,5.16, 5.17, 5.18 MM AgID ABSC 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RI
	MF Authentication	MFA (quali ad es. OTP, smartcard ecc.) implementabili in base al livello di rischiosità dei trattamenti di dati personali e alle prescrizioni delle norme di riferimento. Tra i fattori di autenticazione prevedere anche la possibilità di autenticare anche il singolo device che si collega in relazione alla rischiosità del trattamento.		

Ambito (Da Allegato A – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato A – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato A – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato A – Codice Condotta SW Gestionali)**	**RID**
	Gestione accessi	Adozione di misure che consentono di monitorare e gestire i rischi inerenti agli accessi ai sistemi applicativi, tra cui, a titolo esemplificativo: - disattivazione delle credenziali in caso di inutilizzo per tempi prolungati (es.: sei mesi); - disattivazione temporanea o definitiva in caso di superamento di un numero impostato di tentativi di accesso falliti reiterati; - impostazione di time out della sessione attiva; - visualizzazione data e ora ultimi accessi; - salvataggio dei log di accesso al sistema in modo che i clienti possano esportali a sistemi terzi di conservazione che ne garantiscano l'integrità e la conservazione per i tempi definiti dai clienti stessi		
Profili di accesso	API	- Adozione di misure di autenticazione per le API (es.: certificato digitale; token, ecc.).	ISO/IEC 27002:2022 5.3, 5.1.5, 5.1.6, 5.1.8 MM AgID ABSC 5.1.1, 5.1.2, 5.1.3, 13.9.1 ISO/IEC 29100:2011 5.11	R
	Profili di accesso	Gestione delle utenze, sia utilizzate dal cliente per effettuare attività di amministratori del sistema (ad esempio per essere autonomi nella generazione delle utenze o nell'impostare parametri di utilizzo), sia per l'utilizzo del sistema stesso, in conformità a procedure volte a garantire il rispetto del principio di minimo privilegio e un'adeguata segregazione dei compiti gli utenti devono accedere solo a funzioni, file di dati, URL, controller, servizi e altre risorse, per le quali possiedono un'autorizzazione specifica. Le eventuali utenze generate per far accedere gli incaricati del trattamento del fornitore al fine di prestare assistenza sul prodotto utilizzato saranno identificate nominalmente e avranno profilo di accesso amministrativo e saranno gestite dal cliente con relativa attivazione e disattivazione in caso di necessità di utilizzo.		
Autenticazione	Gestione delle autorizzazioni	Inventario delle utenze presenti nel sistema con i relativi profili di autorizzazione assegnati, disponibile al cliente per sua rendicontazione e analisi degli accessi.	ISO/IEC 27002:2022 5.3, 5.1.5, 5.1.6, 5.1.8 MM AgID ABSC 5.1.1, 5.1.2, 5.1.3, 13.9.1 ISO/IEC 29100:2011 5.11	R
Protezione archivi dati Cliente	Protezione dati Cliente	Adozione di tecniche di pseudonimizzazione o cifratura dei dati (tokenizzazione, etc.) adottabili dal Cliente ove appropriate allo scopo di garantire un adeguato livello di protezione in relazione alle tipologie di dati personali trattati (es.: categorie particolari ex art. 9 del GDPR e dati penali ex art. 10).	ISO/IEC 27002:2022 5.10 MM AgID ABSC 13.3.1 ISO/IEC 29100:2011	RI

Ambito (Da Allegato A – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato A – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato A – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato A – Codice Condotta SW Gestionali)**	**RID**
			5.11	
Protezione archivi	Protezione archivi contenenti le password	Adozione, per la conservazione delle password degli utenti, di adeguate tecniche crittografiche quali le funzioni di derivazione di chiavi crittografiche (Key Derivation Function) che offrono garanzie in caso di loro esfiltrazione dai sistemi informatici del Produttore (cfr. OWASP Password Storage Cheat Sheet, NIST 800-63B Digital Identity Guidelines).	ISO/IEC 27002:2022 8.24	RI
Sicurezza SW	Secure coding	Adozione di policy e procedure finalizzate a garantire che lo sviluppo degli applicativi avvenga nel rispetto di linee guida di secure coding conformi alle best practices (quali, ad es., OWASP, controllo delle librerie di terze parti costante e identificazione di eventuali criticità con segnalazione ai clienti e sostituzione immediata delle librerie che comportano criticità nel trattamento dei dati, etc.).	ISO/IEC 27002:2022 8.25	RI
	Minacce e Vulnerabilità	Test di penetrazione con cadenza periodica (quantomeno al rilascio di ogni major release), se il SW è destinato ad essere esposto su reti pubbliche Adozione di un piano di miglioramento che analizzi le vulnerabilità emerse dai VA e PT e dai bollettini di sicurezza pubblici e di fornitori terzi e ne preveda una adeguata gestione/risoluzione. Svolgimento periodico di analisi di vulnerabilità.	ISO/IEC 27002:2022 8.8 MM AgID ABSC MM AgID ABSC 4.1.1, 4.1.2, 4.4.2, 4.6.1 ISO/IEC 29100:2011 5.11	RID
Requisiti sistemistici e di gestione	Log applicativi di attività utente	Funzionalità per il tracciamento del log degli accessi e delle attività svolte in relazione alle diverse tipologie di utenza (amministratore, super utente, utente, etc.) allo scopo di consentire al titolare o al responsabile del trattamento un'adeguata attività di monitoraggio. I log riguardanti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore del sistema del Cliente.	ISO/IEC 27002:2022 8.15 MM AgID ABSC 5.4.1, 5.1.1	RID
Ambienti di test	Misure per ambienti di test	Separazione degli ambienti di test e sviluppo rispetto ad ambienti di produzione e previsione di misure di accesso mediante credenziali e privilegi diversi in modo di ridurre al minimo i rischi.	ISO/IEC 27002:2022 8.31, 8.33 MM AgID ABSC 4.10.1, 8.2.3	RI
Funzioni specifiche	Data retention	Previsione di funzioni del SW che consentano ai clienti di impostare la cancellazione dei dati personali trascorso il periodo necessario di loro conservazione. Il SW deve prevedere estrazioni di dati che consentano ai clienti di essere consapevoli sui periodi di conservazione dei dati al fine di trattare i dati secondo il principio di minimizzazione.	ISO/IEC 27701:2019 A.7.4.7	RID

Ambito (Da Allegato A – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato A – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato A – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato A – Codice Condotta SW Gestionali)**	**RID**
Funzioni specifiche	Portabilità	Funzionalità idonee a consentire al Cliente l'estrazione dei dati personali in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo in caso di esercizio del diritto alla portabilità da parte dell'interessato, ove ne ricorrano i presupposti.	GDPR art. 20	D
Misure organizzative	Formazione	Erogazione periodica alle persone autorizzate al trattamento di corsi di formazione sulla sicurezza e protezione dei dati personali. Per gli sviluppatori sono previsti anche corsi di sviluppo sicuro.	ISO/IEC 27002:2022 6.3 MM AgID ABSC 8.7.2, 8.7.3, 8.7.4	RID
Misure di sicurezza	Backup	Funzionalità al fine di permettere al Cliente di effettuare, anche tramite processi esterni, il salvataggio o backup dei dati trattati dall'applicativo.	ISO/IEC 27002:2022 8.13 MM AgID ABSC 10.1.2 ISO/IEC 29100:2011 5.11	ID
Misure di sicurezza	Esattezza e accuratezza dei dati	Adozione di misure per assicurare al Cliente una verifica dell'esattezza e dell'accuratezza dei dati (ad es. controlli di correttezza formale della PIVA o CF).	ISO/IEC 27701 A.7.4.3	RI
Misure di sicurezza	Riservatezza dei dati	Adozione di misure per agevolare il Cliente nel rispetto del requisito della riservatezza in caso di utilizzo di funzioni di condivisione dei dati (tramite ad es. l'invio di avvisi o notifiche).	ISO/IEC 27701 A.7.4.3	R
Misure organizzative	Inventory Librerie	Conservazione dell'inventario delle componenti software in uso comprensive delle librerie di terzi e/o open source in modo da poter rispondere più tempestivamente in caso di segnalazioni di vulnerabilità (SBOM SW bill of materials).	ISO/IEC 27002:2022 5.6, 8.4 MM AgID ABSC 2.1.1	RID
Misure organizzative	Change management	Regolamentazione del processo di gestione delle modifiche applicative ed infrastrutturali, al fine di garantire un miglior presidio di ogni fase del ciclo di vita del SW e di tracciarne l'evoluzione, con monitoraggio dei livelli di accesso alle informazioni critiche e adeguata formazione/sensibilizzazione delle persone coinvolte nel processo di Change Management (al rispetto dei principi di *Segregation of Duties*).	ISO/IEC 27002:2022 5.3, 8.32	D
Misure organizzative	Configuration management	Regolamentazione del processo di Configuration management al fine di garantire la corretta gestione delle versioni dei rilasci dei moduli SW.	ISO/IEC 27002:2022 8.9	RID
Misure di sicurezza	Trasmissione dati personali	Utilizzo di protocolli sicuri e adeguati allo sviluppo tecnologico per proteggere i dati durante la loro trasmissione.	ISO/IEC 27002:2022 5.10, 5.14, 8.26 ISO/IEC 27701:2019 A.7.4.9	RI

Ambito (Da Allegato A – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato A – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato A – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato A – Codice Condotta SW Gestionali)**	**RID**
			Misure Minime AgID ABSC 3.3.2 ISO/IEC 29100:2011 5.11	
Misure di sicurezza	File temporanei	Funzionalità per permettere l'eliminazione dei file temporanei contenenti dati personali e creati durante i trattamenti e cancellazione sicura dei dati sugli strumenti dismessi (*Secure disposal*).	ISO/ISO 27701: A.7.4.6	R

ANNESSO 2 – Misure di sicurezza da applicare per sistemi gestiti dall'appaltatore presso il data center locale.

Ambito (Da Allegato B – on premise – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**RID**
Gestione Account	Autorizzazione e autenticazione	Tutti gli operatori della SWH devono accedere alle piattaforme utilizzate per l'assistenza previa autenticazione con le credenziali nominative individuali. Nel caso di un tentativo d'accesso alla piattaforma di supporto con un account diverso da quello autorizzato, il sistema deve negare l'accesso. Le Utenze degli operatori incaricati dell'assistenza sono periodicamente revisionate allo scopo di verificare che i permessi e le autorizzazioni di accesso siano sempre aggiornate.	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18 MM AgID ABSC 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RID
	Assegnazione privilegi	L'assegnazione dei privilegi agli operatori deve avvenire in base al principio del "need-to-know" e della "segregation of duties".		
	Password policy	Le password di accesso degli operatori incaricati dell'assistenza devono essere composte da almeno dodici (12) caratteri, prevedere caratteri alfanumerici e caratteri speciali, essere sostituite almeno ogni novanta (90) giorni, qualora si tratti di utenze privilegiate nella configurazione del SW, e conservate in formato crittografato.		
	Utilizzo della VPN	L'erogazione del servizio di assistenza e di accesso alla piattaforma da remoto devono avvenire mediante connessione VPN con MFA. La VPN può essere del Cliente o configurata dalla SWH in accordo col Cliente; prima dell'utilizzo di ogni sessione ci deve essere l'autorizzazione del Cliente che deve attivare o disattivare l'accesso ai propri sistemi in relazione alle attività svolte e richieste dallo stesso. Al termine dell'intervento l'operatore di assistenza dovrà comunicare al Cliente la fine dell'intervento e richiedere la disattivazione dell'accesso	ISO/IEC 27002:2022 8.21	RID
Gestione Sicurezza Logica	Patch Management	Continuo patching applicativo di sicurezza relativo alla piattaforma per l'erogazione del supporto da remoto.	ISO/IEC 27002:2022 8.8	RID
Log Management	Monitoraggio e gestione dei log di attività	Le attività svolte dagli operatori con utenze privilegiate devono essere tracciate e monitorate.	ISO/IEC 27002:2022 8.15 MM AgID ABSC 5.4.1, 5.1.1	R

Ambito (Da Allegato B – on premise – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**RID**
Supporto da remoto in modalità attended (con presidio di un soggetto autorizzato da parte del Cliente)	Gestione dell'escalation interna	Gli operatori incaricati dell'assistenza devono accertarsi che le richieste di assistenza provengano da un soggetto identificato e preventivamente autorizzato dal Cliente (ad esempio tramite autenticazione sulla piattaforma di ticketing).	ISO/IEC 27002:2022 5.16 ISO/IEC 29100:2011 5.11	RID
	Gestionedel sistema di supporto	Gli operatori incaricati dell'assistenza devono richiedere al Cliente in modo tracciabile le autorizzazioni necessarie ai fini dell'erogazione del servizio di assistenza (ad esempio, la condivisione dello schermo, il controllo condiviso dell'applicativo, il trasferimento dei file e la registrazione delle attività).	NA	R
Supporto da remoto in modalità unattended	Assegnazione dei privilegi da parte del Cliente	Deve essere garantita al Cliente la possibilità di assegnare specifici diritti ai determinati operatori incaricati dell'assistenza al fine di limitare l'accesso ai propri sistemi solo al personale autorizzato e per un intervallo temporale definito.	ISO/IEC 27002:2022 5.15,5.16 ISO/IEC 29100:2011 5.11	R
Supporto da remoto in modalità unattended	Accesso al DB	L'accesso agli ambienti di produzione da parte di Utenti che non operano in qualità di amministratori di sistema è consentito unicamente in presenza di comprovate esigenze di assistenza/manutenzione e mediante un processo autorizzativo ad hoc che consenta di tracciare la richiesta/autorizzazione del Cliente (es. "trouble ticketing").	ISO/IEC 27002:2022 5.15,5.16, 5.17, 5.18 MM AgID ABSC 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RI
Attività di test	Utilizzo dei dati per l'esecuzione dei test	Utilizzo di dati fittizi (non dati reali) per l'esecuzione dei test. Solo in casi particolari, su richiesta del Cliente, ed in particolare quando sono sviluppate funzioni particolarmente complesse che devono essere provate e che devono essere verificate sull'esattezza della singola elaborazione e del singolo interessato presente negli archivi, prima di utilizzare gli archivi viene verificata l'adozione delle misure di sicurezza presenti negli ambienti di produzione. In questi casi i dati devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di verifica della qualità e poi cancellati.	ISO/IEC 27002:2022 5.10	

Ambito (Da Allegato B – on premise – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**RID**
	Accesso agli ambienti dei Clienti tramite IP pubblici	Il collegamento tramite IP pubblici su ambienti cloud dovrà avvenire da parte degli operatori incaricati dell'assistenza con utenze individuali, che dovranno essere attivate dal Cliente al fine di evadere la richiesta di assistenza. Solo nel caso in cui è previsto un servizio di assistenza continuativo tali credenziali potranno rimanere sempre attive, ma in questo caso gli accessi degli operatori dovranno essere loggati e l'operatore per ogni intervento dovrà giustificare la finalità per cui l'ha dovuto effettuare. Per tale finalità l'ambiente applicativo potrà prevedere utenze precaricate a sistema e le procedure di assegnazione delle stesse saranno in carico alla SWH in relazione alle esigenze segnalate dal Cliente.	ISO/IEC 27002:2022 5.15, 5.16, 5.17, 5.18 ISO/IEC 29100:2011 5.11	R
Gestione archivi	Autorizzazione per copia/trasferimento dati temporanei	L'eventuale copia o trasferimento di archivi o base dati del Cliente per finalità di assistenza o manutenzione deve essere preventivamente ed espressamente autorizzata dal Cliente stesso.	ISO/IEC 27002:2022 5.14	RI
	Secure disposal	I DB/archivi del Cliente devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di assistenza e immediatamente cancellati qualora non più necessari per l'esecuzione delle operazioni di assistenza.	ISO/ISO 27701: A.7.4.6	R
		Le copie dei DB/archivi del Cliente prelevati per finalità di assistenza devono essere trasferite tramite canali sicuri e protetti, salvate in ambienti dotati delle opportune misure di sicurezza e non devono essere sottoposti a backup allo scopo di minimizzare il trattamento.	ISO/IEC 27002:2022 5.14, 8.26 ISO/IEC 27701:2019 A.7.4.9	R
	Secure disposal	Qualora durante le attività di assistenza fosse necessario stampare documenti o informazioni, tali documenti devono rimanere nell'esclusiva disponibilità dell'operatore e da questi devono essere protetti contro accessi non autorizzati. Al termine dell'attività, i documenti dovranno essere distrutti.	ISO/ISO 27701: A.7.4.6	R

Ambito (Da Allegato B – on premise – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – on premise – Codice Condotta SW Gestionali)**	**RID**
	Attività di Migrazione e conversione	In relazione alle attività di migrazione dei dati sono da prevedere le seguenti misure di sicurezza: - Utilizzo di canali sicuri e protetti nella trasmissione dei dati; - Utilizzo delle basi dati contenenti dati effettivi in ambiente dedicato, dotato di misure di sicurezza idonee a garantirne la riservatezza; - Configurazione dei profili di accesso a tali ambienti al solo personale preposto dalla SWH alla gestione delle attività di migrazione compreso il test ed il collaudo. Ove richiesto, tali profili sono estesi anche al personale del Cliente. Qualora presenti, gli accessi da remoto avvengono sempre mediante l'utilizzo di canali sicuri; - Conservazione dei dati esclusivamente fino al buon fine del completamento delle attività di verifica ed alla conseguente consegna, approvazione e accettazione da parte del Cliente.	ISO/IEC 27002:2022 5.14, 5.15, 8.26 ISO/IEC 27701:2019 A.7.4.9	RI
Governance	Tracciabilità	Sono adottati processi e strumenti di assistenza che assicurino la tracciabilità degli interventi richiesti ed eseguiti (piattaforma di ticketing).	ISO/IEC 27002:2022 5.10	RID
Governance	Data Breach	Sono adottate procedure di gestione degli incidenti che consentono di individuare, contenere e risolvere situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.	ISO/IEC 27002:2022 5.5, 5.24, 5.25, 5.26, 5,27	RID

ANNESSO 3 – Misure di sicurezza da applicare per sistemi gestiti dall'appaltatore presso un data center sotto il controllo dell'appaltatore.

Ambito (Da Allegato B – in cloud – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**RID**
Misure sicurezza Data Center	Accesso al Sistema o SW (autenticazione)	Adozione di misure dirette a garantire che: - gli accessi di amministrazione da parte della SWH siano riservati al personale a cui sia attribuita la qualifica ("ruolo") di amministratore di sistema, in virtù di elevate capacità tecniche e caratteristiche di comprovata affidabilità e moralità ; - l'accesso amministrativo ai sistemi da parte del personale del Cliente avverrà attraverso procedure di autenticazione a più fattori (MFA).	ISO/IEC 27002:2022 5.15, 5.16, 5.17, 5.18, 8.15 MM AgID ABSC 5.1.1, 5.4.1, 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RID
isure sicurezza Data Center	Accesso al Sistema o SW (policy di gestione)	Per i servizi che prevedono una modalità di gestione amministrativa delle componenti infrastrutturali, devono essere previste le seguenti policy: - utenze che consentono l'individuazione dell'amministratore che esegue l'intervento; - attivazione di un processo di log management che identifichi i log in, log out e log in failed; - conservazione dei log in un formato che ne garantisca l'integrità e la lettura nel tempo; - conservazione dei log per almeno sei (6) mesi; - verifica annuale dell'operato degli amministratori di sistema; - accesso ai sistemi attraverso VPN e MFA.	ISO/IEC 27002:2022 5.3	

Ambito (Da Allegato B – in cloud – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**RID**
Misure sicurezza Data Center	Log Management	Funzionalità per il tracciamento o registrazione (log) degli accessi e delle attività svolte dagli Utenti. I log concernenti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore di sistema del Cliente o della Software House su richiesta del Cliente.	ISO/IEC 27002:2022 8.15	R
Misure sicurezza Data Center	Auditing	Utilizzo del sistema di gestione e analisi dei log anche per il monitoraggio delle attività degli amministratori di sistema. L'accesso al sistema di gestione dei log è riservato al personale avente ruolo di auditor e non è ammesso per il personale addetto all'amministrazione di sistema.	ISO/IEC 27002:2022 8.16	R
Misure sicurezza Data Center	Crittografia dei protocolli di comunicazione	Applicazione di protocolli crittografici standard di comunicazione sicuri e non obsoleti, nei casi in cui l'accesso al sistema sia effettuato tramite Internet.	ISO/IEC 27002:2022 5.14, 8.21 ISO/IEC 29100:2011 5.11	RI
Misure sicurezza Data Center	Minacce e Vulnerabilità	Adozione di un programma di gestione delle minacce e dei rischi per monitorare continuamente le vulnerabilità delle Piattaforme SaaS indicate da best practice internazionali attraverso la pianificazione e l'esecuzione di scansioni delle vulnerabilità interne ed esterne e test di penetrazione. Le vulnerabilità identificate devono essere valutate per determinare i rischi associati e le opportune azioni correttive stabilite in base alla priorità assegnata e gravità rilevata.	ISO/IEC 27002:2022 8.8 MM AgID ABSC MM AgID ABSC 4.1.1, 4.1.2, 4.4.2, 4.6.1 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Firewalling	Adozione di sistemi di firewall finalizzati a filtrare e contenere il traffico identificando eventuale traffico anomalo indicatore di possibili attacchi informatici. Presenza di firewall L4 o L7/WAF.	ISO/IEC 27002:2022 5.14, 8.22 ISO/IEC 29100:2011 5.11	RID Res

Ambito (Da Allegato B – in cloud – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**RID**
Misure sicurezza Data Center	Intrusion Prevention	Protezione dell'ambiente mediante cui è erogato il servizio dalla SWH mediante Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito.	ISO/IEC 27002:2022 7.4, 8.21 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Malware protection	Adozione di misure di protezione da infezioni di software malevolo, di difesa da azioni non autorizzate, da applicazioni sospette e di protezione da tentativi di sottrazione di dati personali (es. mediante sistemi antivirus, antispamming, antiphishing, etc., mantenuti costantemente aggiornati).	ISO/IEC 27002:2022 8.7 MM AgID BSC 8 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Filesystem Antivirus	Adozione di moduli Antivirus sul filesystem su tutti i server utilizzati per la fornitura dei servizi, con possibilità di configurare, su base progettuale, prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.	ISO/IEC 27002:2022 8.7 MM AgID ABSC 8 ISO/IEC 29100:2011 5.11	RD
Misure sicurezza Data Center	Monitoraggio e gestione incidenti	Adozione di policy e procedure per l'identificazione, gli interventi, i rimedi e le segnalazioni di incidenti che determinano un rischio per l'integrità o riservatezza dei dati personali o altre violazioni della sicurezza.	ISO/IEC 27002:2022 5.24, 5.25, 5.26, 5.27, 5.28, 6.8	RID Res
Misure sicurezza Data Center	Security Patch Management	Sottoposizione della piattaforma ad un processo periodico di verifica delle patch o delle fix disponibili relativamente alle componenti dell'impianto di erogazione e a quelle ritenute critiche per l'erogazione del servizio o per la sicurezza.	ISO/IEC 27002:2022 8.8 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Sicurezza fisica	Applicazione di adeguate misure di sicurezza fisica alla piattaforma hardware/software progettata (es. utilizzo di hosting providers/servizi di data center dotati di adeguati sistemi di prevenzione del rischio intrusione, incendio, allagamento, ecc.).	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res

Ambito (Da Allegato B – in cloud – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**RID**
Misure sicurezza Data Center	Anti allagamento	Adozione nell'ambito del Data Center di tutte le misure necessarie a prevenire allagamenti (quali presenza di sonde, impianti di allarme, ecc.).	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res
Misure sicurezza Data Center	Anti intrusione	Impostazione nel Data Center di un sistema di controllo degli accessi che identifichi coloro che accedono e impedisca l'accesso ai non autorizzati. La procedura deve prevedere anche la gestione del Change con l'attivazione e disattivazione dell'autorizzazione all'accesso in funzione dei cambi di ruolo.	ISO/IEC 27002:2022 7.1, 7.2 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Telecamere a circuito chiuso	Installazione di telecamere (CCTV) per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.	ISO/IEC 27002:2022 7.4 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Condizionamento	Adozione di adeguati impianti di condizionamento e di raffreddamento degli ambienti ed apparati.	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res
Misure sicurezza Data Center	Continuità ed emergenza	Adozione di procedure e controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema/SW (in caso di incidente / violazione di dati personali). Le procedure devono comprendere le indicazioni per la conservazione delle copie di backup nonché un piano per il disaster recovery.	ISO/IEC 27002:2022 5.4, 5.29 MM AgID ABSC 10 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Cancellazione dei dati	Previsione di misure per la cancellazione dei dati di produzione al termine dell'erogazione del servizio secondo i termini contrattuali definiti con il Cliente.	ISO/IEC 27002:2022 8.10	R
Misure sicurezza Data center esterni	Verifica dei requisiti del sub-fornitore e contrattualizzazione degli obblighi relativi alle misure di sicurezza	Selezione e verifica dei requisiti del sub-fornitore che assume la gestione sistemistica dei server e dell'infrastruttura necessari allo svolgimento dei Servizi e sottoscrizione di un contratto che vincoli il medesimo sub-fornitore al rispetto degli obblighi concernenti le misure di sicurezza (previsti dalla SWH per la gestione del DC).	ISO/IEC27002:2022 5.19; 5.20	RID

Ambito (Da Allegato B – in cloud – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**RID**
Misure sicurezza Data center esterni	Audit nei confronti del sub-fornitore	Sottoposizione del sub-fornitore che gestisce il DC esterno ad audit periodici per la verifica del rispetto degli obblighi concernenti le misure di sicurezza, fatto salvo quanto previsto dalle condizioni di servizio fissate da providers multinazionali di servizi di DC ai sensi dell'art. 7.7 del CoC.	ISO/IEC 27002:2022 5.22	RID
Connettività	Linee Internet e disponibilità di banda	Previsione di misure volte ad assicurare una connettività adeguata in conformità ai livelli di servizio contrattualmente definiti con il Cliente.	ISO/IEC 27002:2022 8.6, 8.21	RI
Connettività	Firewalling	Protezione dell'accesso ai sistemi contro il rischio d'intrusione attraverso adeguate misure di firewalling.	ISO/IEC 27002:2022 5.14, 8.22, 8.21, 8.23 ISO/IEC 29100:2011 5.11	RID
Sicurezza rete	AntiDDoS	Erogazione da parte del Data Center di un servizio in grado di rispondere in modo efficace alle problematiche create dagli attacchi ("**DDoS**").	ISO/IEC 27002:2022 8.20 ISO/IEC 29100:2011 5.11	D
Sicurezza rete	IDS/IPS	Adozione di un sistema IPS (Intrusion Prevention System) in grado di bloccare automaticamente gli attacchi rilevati e IDS (Intrusion Detection System) in grado di intercettare le minacce fornendo così una protezione real-time ai servizi erogati dal Data Center.	ISO/IEC 27002:2022 8.20 ISO/IEC 29100:2011 5.11	RD
Governance	Formazione	Erogazione periodica di corsi di formazione sulla sicurezza e protezione dei dati personali ai propri dipendenti coinvolti nelle attività di trattamento.	ISO/IEC 27002:2022 6.3	na
Governance	Ubicazione geografica	Dichiarazione da parte della SWH nei confronti del Cliente dell'ubicazione geografica del DC e dei dati.	ISO/IEC 27002:2022 5.31	na
Governance	Data Breach	Adozione di procedure di individuazione, contenimento e risoluzione di situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.	ISO/IEC 27002:2022 5.5, 5.24, 5.25, 5.26, 5,27	RID

Ambito (Da Allegato B – in cloud – Codice Condotta SW Gestionali)	**Catalogazione (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Requisito di dettaglio (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**Riferimenti (Da Allegato B – in cloud – Codice Condotta SW Gestionali)**	**RID**
Requisiti sistemistici e di gestione	Sicurezza logica	Rivalutazione con cadenza almeno annuale delle misure e procedure di sicurezza applicate in modo da aggiornarle in relazione alle vulnerabilità rilevate, agli attacchi subiti e all'evoluzione della tecnologia.	ISO/IEC 27002:2022 8.27 MM AgID ABSC 3.1.2	RI

ANNESSO 4 – ALTRE MISURE DI SICUREZZA

Le misure attivate al trattamento sono:

- *misure di pseudonimizzazione e cifratura dei dati personali (obbligatoria a livello di campo per sistemi che gestiscono categorie di dati particolari e per dati giudiziari):*
  - *il gruppo di progetto deve utilizzare una crittografia a livello di hard-disk sui sistemi utilizzati;*
  - *il prodotto sviluppato può utilizzare solo crittografia nelle modalità indicate dalla linea guida dell'ACN valida al momento del rilascio;*
  - *è necessario consegnare specifico documento con cui si spiegano le modalità di gestione della crittografia sulla soluzione consegnata;*
  - *è necessario consegnare documento specifico sulla gestione delle chiavi crittografiche;*
  - *è opportuno utilizzare solo librerie di funzioni crittografiche certificate o provenienti da fonti note e tracciabili;*
  - *utilizzo di certificati di sicurezza (di certification autority) concordati con LAZIOcrea per la gestione della comunicazione fra sistemi diversi.*

- *misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento:*
  - *il gruppo di progetto deve consegnare specifici documenti che indichino:*
    - *elenco degli amministratori di sistema aggiornato;*
    - *le evidenze sui controlli semestrali effettuati dal titolare sgli amministratori di sistema (secondo le definizione del Provvedimento dell'Autorità Garante di cui al https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499;*
      annotazione: nel caso di sistemi applicativi complessi occorre declinare i controlli sui soli soggetti autorizzati che hanno possibilità di effettuazione di azioni di controllo sull'operato di altri utenti e limitatamente agli autorizzati dell'appaltatore tenendo definendo in apposito documento eventuali limiti di comportamento secondo proposta del appaltatore sottoposta per approvazione al PM/RUP/Gestore entro 30 giorni dall'inizio delle attività;
    - *analisi dei rischio privacy del gruppo di progetto in funzione del RID (Riservatezza, Integrità, Disponibilità);*
    - *struttura dei profili utente del gruppo di progetto;*
    - *modalità di gestione dei dati personali da parte del gruppo di progetto;*
    - *modalità di applicazione della profilatura Accessi sistemi e DB (Segregation of duty, need to know e last privilege) del gruppo di progetto;*
    - *modalità di erogazione della formazione al gruppo di progetto;*
    - *evidenze delle istruzioni fornite e della formazione effettuata al personale del gruppo di progetto.*

  Inoltre occorre fornire a tutti i partecipanti del gruppo di progetto le seguenti regole organizzative di tutela:
    - *non effettuare trattamenti che possano in qualunque modo impattare sulla riservatezza, disponibilità o confidenzialità dei dati del LAZIOcrea;*
    - *non esportare su chiavetta o altro supporto dati prelevati dai sistemi, dai database o dai server sotto il controllo di LAZIOcrea;*
    - *non installare applicativi o tool web sulle postazioni lavorative di LAZIOcrea;*
    - *non modificare in nessun modo le configurazioni delle risorse informatiche a meno di approvazione esplicita di LAZIOCrea.*

Per la soluzione progettata consegnare specifici documenti che riportino:

- *architettura della soluzione e le sue parte (comprensive delle versioni delle singole componenti);*
- *analisi del rischio privacy del prodotto progettato/consegnato in funzione del RID con riferimento privacy (Riservatezza, Integrità, Disponibilità);*
- *modalità di gestione delle utenze di accesso ai Data Base (con particolare attenzione alle utenze di accesso di data base di altri sistemi già in essere) (si consiglia la produzione di un documento in cui si elenchino tutte le utenze di accesso ad altri data-base e il motivo dell'utilizzo del sistema esterno) ;*
- *struttura dei profili utente applicativo;*
- *profilatura accessi sistemi e DB (Segregation of duty, need to know e last privilege):*
- *presenza di una funzione di log differenziato per ruolo utente;*
- *presenza di funzioni atte alla cancellazione di utenti o di profili.*

- *misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico:*

Per il gruppo di progetto

- *sistemi di backup del progetto in corso;*
- *consegna di documenti che descrivano le modalità di attuazione di:*
  - *sistemi di backup del gruppo di progetto e dei siti di sviluppo e test;*
  - *gestione del backup delle installazioni di sviluppo e test;*
  - *utilizzo di cloud (autorizzato ai sensi del Capo V del GDPR);*
  - *gestione del versioning delle parti software in fase di sviluppo/test.*

Per la soluzione progettata

- *gestione del versioning delle parti sviluppate;*
- *politiche di backup della soluzione applicativa (RPO, RTO, metodologie consigliate);*
- *definizione degli script di backup nel rispetto delle procedure interne sottocitati;*
- *La soluzione deve in ogni caso rispettare quanto specificato su:*
  - *PRO_SGSI_ A.12.3 " Processo e Politica di Gestione di Backup e Data Retention*

NOTA: In caso di gestione di una applicazione già in ambiente di esercizio di LAZIOcrea occorre dare evidenza del rispetto delle prescrizione in essere in LAZIOcrea s.p.a. relative a Sicurezza Informatica, Privacy e Risk Manager Aziendale.

- *procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento:*
  - *consegna di documenti che evidenzino:*
    - *attività di restore del gruppo di progetto;*
    - *prescrizioni sul restore della soluzione applicativa;*
    - *rapporti audit interni con cadenza almeno annuale al gruppo di progetto;*
    - *rapporti di audit sulla funzioni di amministrazione di sistema di tutta la filiera controllata;*
  - *audit esterni da parte di LAZIOcrea o da soggetti da lei individuati nel rispetto delle prescrizioni della clausola 7.6.;*
  - *l'affidatario è tenuto alla effettuazione di un vulnerability assessment/penetration test sulla soluzione così come inserita in ambiente di prova (prepoduzione). A seguito del VA/PT deve consegnare il report emesso comprensivo del remediation plan che è tenuto ad applicare.*

- *misure di identificazione e autorizzazione dell'utente consegna di documenti che evidenzino:*
  Per il gruppo di progetto
  - *profili utente per l'accesso al progetto;*
  - *autenticazione con sistemi di autenticazione multifattoriale;*

  Per la soluzione progettata rispetto di quanto definito in ANNESSO 1 ed inoltre:
  - *utilizzo dello IAM Centralizzato disponibile su LAZIOcrea (Identity and Access Management);*
  - *rispetto delle specifiche presenti nel documento di Specifica Tecnica: "Integrazione applicativa dei servizi d'autenticazione SPID, CieID e TS-CNS via SAML 2.0 - Web SSO e OAuth-OpenID", o meccanismi previsti dalla Linee Guida ACN ove più recenti.*

- *misure di protezione dei dati durante la trasmissione consegna di documenti che evidenzino, per la soluzione progettata e per gli scambi del gruppo di progetto le modalità di utilizzo di:*
  - *protocollo Https;*
  - *protocolli TLS 1.2 o successivi;*
  - *FTPS o SFTP per il trasferimento di file;*
  - *accesso all'ambiente LAZIOcrea attraverso VPN o resa disponibile dal fornitore o utilizzando quella disponibile sul data center di LAZIOcrea (limitare il tempo di connessione continuativo attraverso VPN ad un massimo di massimo 5 ore);*
  - *utilizzo di certificati di sicurezza concordati con LAZIOcrea per la gestione della comunicazione fra sistemi (ivi compresa la documentazione di definizione ed utilizzo di tali certificati – I certificati devono essere ridondati e provenienti da almeno di certification autority riconosciute da ACN/AgID.*
  - *descrizione ed elencazione dei cookie utilizzati e motivazione dell'utilizzo;*
    Attenzione i cookie di google analytcs non sono utilizzatili, preferire sistemi MATOMO o in ogni caso open source o chiedere soluzione specifica AgID per le pubbliche amministrazioni;

- *misure di protezione dei dati durante la conservazione:*
  Per il gruppo di progetto:
  - *conservazione in armadi chiusi a chiave del supporto cartaceo;*
  - *server di conservazione con accesso riservato con credenziali utente;*
  - *sviluppo dell'applicazione su sistemi protetti con antivirus, antispam;*
  - *ambiente di sviluppo protetto da firewall;*
  - *crittografia dei dischi del gruppo di progetto (specie se opera con portatili);*
  - *tracciamento degli accessi ai dati di progetto;*

  Per la soluzione progettata:
  - *tracciamento dell'accesso ai dati (consegna di documento esplicativo specifico);*
  - *crittografia dei dischi (consegna di documento esplicativo specifico nel rispetto delle linee guida ACN);*
  - *crittografia di ambito o a livello di campo a seguito di valutazione di quale tecnologia rispetti il contesto applicativo (consegna di documento esplicativo specifico nel rispetto delle linee guida ACN) compresa documentazione di certificazione della soluzione adottata;*
  - *IPS (Intrusion prevention systems);*

- *Metodologie di protezione dei dati di Test forniti da LAZIOCrea ivi compreso l'utilizzo di specifiche password e elenco dei soggetti autoritzzzati all'uso di tali dati di test.*

La soluzione deve in ogni caso rispettare quanto specificato su:

a. *PRO_SGSI_7.5 "Processo e Politica per la Gestione della Documentazione e delle Registrazioni";*
b. *PRO_SGSI_A.10 "Processo e Politica di Gestione della Crittografia*
c. *Installazione in ambiente*
   - *dotato di IPS (Intrusion prevention systems)*
   - *inserito in Reti LAN opportunamente segregate*

- *misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati:*

Per il gruppo di progetto occorre documentare opportunamente:

- *misure di Anti-Intrusione degli ambienti di lavoro;*
- *sistema Anti-incendio, specie nei luoghi dove sono presenti attrezzature che permettono il funzionamento del gruppo di progetto e della soluzione in fase di sviluppo;*
- *metodologie di accesso Fisico ai luoghi di progetto regolamentato anche per terze parti, ospiti e visitatori;*
- *misure di sicurezza fisica del gruppo di progetto;*

La soluzione sarà ospitata su un ambiente dotato di:

- *misure Anti-Intrusione degli ambienti di lavoro;*
- *sistema di Videosorveglianza;*
- *sistema Antincendio;*
- *sistemi di Continuità Elettrica;*
- *spazi protetti dall'accesso;*
- *accesso Fisico Regolamentato anche per terze parti, ospiti e visitatori.*

La soluzione deve in ogni caso rispettare quanto specificato su:

a. *PRO_SGSI_A.11 Processo e politica di gestione della Sicurezza Fisica e Ambientale"*

- *misure per garantire la registrazione degli eventi:*

Per il gruppo di progetto:

- *sistemi di log per le attività del gruppo di progetto;*
- *conservazione di log per non meno di 180 giorni;*
- *log specifici per gli amministratori di sistema;*
- *evidenze dei controlli periodici sui log;*
- *log accedibiili in fase di audit di verifica e controllo;*
- *disponibilità di una procedura di gestione degli incidenti;*

Per la soluzione progettata:

- *sistema di raccolta degli eventi (LOG) relativi a particolari operazioni sul sistema (ad esempio: creazione utenti applicativi, creazione ruoli, conflitti sui ruoli attribuiti agli utenti,…)*
- *inalterabilità dei log generati;*
- *report sui log (in particolar modo sull'utilizzo delle utenze riservate e/o amministrative);*
- *conservazione dei LOG per non meno di 180 giorni (consegnare documento esplicativo);*

La soluzione sarà ospitata su un ambiente dotato di gestione degli accessi IAM sottoposto a proprio LOG (limitato all'accesso).
La soluzione deve in ogni caso rispettare quanto specificato su:

b. *PRO_SGSI_ A.A.12.4 " Processo e politica di gestione di Log e Monitoraggio"*

- *misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita*

Per il gruppo di progetto:

- *documenti progettuali per descrivere la struttura dell'ambiente di sviluppo;*
- *documenti progettuali per descrivere la struttura dell'ambiente di test e di produzione (tale documento permetterà la predisposizione all'interno degli ambienti operativi di LAZIOCrea)*

Per la soluzione progettata:

- *documento di configurazione (dettagliata delle singole parti comprese le versioni utilizzate) del prodotto consegnato/da consegnare;*
- *documento di vincoli alla configurazione e modalità di aggiornamento e risoluzione di vulnerabilità note;*
- *documento di configurazione delle librerie software utilizzate;*
- *documento e routine di configurazione/creazione degli spazi data base;*
- *documento di analisi dei rischi della soluzione*
- *server e apparati di infrastruttura (se previsti) configurati secondo Best Practice di Settore (con documentazione di configurazione);*
- *documenti di verifica del rispetto delle linee guida rese disposnibili da ACN/AgID sull'argomento.*

- *misure di informatica interna e di gestione e governance della sicurezza informatica:*

Per il gruppo di progetto:

- *referente della sicurezza di progetto;*
- *piani di formazione ed evidenze della formazione erogata in ambito privacy con cadenza almeno annuale del personale coinvolto nel progetto;*
- *contratti esterni da sub-responsabile a struttura identificata e autorizzata;*

Per la soluzione progettata:

- *istruzioni per gli Amministratori di sistema di applicativo complesso;*
- *reportistica mirata all'utilizzo del sistema;*
- *routine di cancellazione sicura;*
- *reportistica di cancellazione sicura (compresa attestazione di avvenuta cancellazione);*
- *procedure di sviluppo sicuro secondo specifiche di prodotto AgID;*
- *gestione dei collegamenti sicuri a eventuali servizi esterni all'applicazione (quadro sinottico, documento per specificare i protocolli e le modalità del colloquio);*
- *elenco delle utenze necessarie a garantire il colloquio con altri sistemi (documento riservato con indicazioni della modalità utilizzata per gestire le utenze di colloquio);*

La soluzione deve in ogni caso rispettare quanto specificato sull'ANNESSO 1

- *misure di certificazione/garanzia di processi e prodotti*
  - *la soluzione deve essere certificabile ai sensi dell'art. 42 del GDPR;*

- *la soluzione deve essere sottoponibile a certificazione nell'ambito del contesto di riferimento (ad esempio certificazione di prodotto sanitario);*
- *nel caso di ambiti specifici la soluzione deve possedere le certificazioni di ambito prima della consegna al collaudo.*

- *misure per garantire la minimizzazione dei dati (verificare quanto definito in ANNESSO 1)*
  - *analisi in modalità privacybydesign privacybydefault (documentata)*
  - *raccolta collegata al rispetto di normative vigenti (documentata)*

- *misure per garantire la qualità dei dati (verificare quanto definito in ANNESSO 1):*
  - *utilizzo di routine di individuazione di data leak (documentate);*
  - *presenza di verifiche con altri sistemi esterni;*
  - *controllo intrinseco sulla conformità del dato inserito;*
  - *gestione dei collegamenti sicuri ai servizi esterni coinvolti nelle verifiche.*

- *misure per garantire la conservazione limitata dei dati (verificare quanto definito in ANNESSO 1):*
  - *Per il gruppo di progetto:*
    - *impegno contrattuale;*
    - *attestazione di fine trattamento con cancellazione entro un massimo di 90 giorni dal termine del progetto;*
    - *documento che descriva la procedure si cancellazione sicura al termine del trattamento.*

- *misure per garantire la responsabilità:*
  - *Per il gruppo di progetto:*
    - *organigramma privacy del gruppo di progetto;*
    - *individuazione di un DPO del gruppo di progetto;*
    - *attribuzione delle stesse misure applicabili ai soggetti esterni che operano come sub-responsabili del trattamento (evidenza da mostrare in audit).*

- *misure per consentire la portabilità dei dati e garantire la cancellazione (verificare quanto definito in ANNESSO 1):*
  - *procedure (anche software) di selezione dei dati ed esportazione verso file csv (Comma-separated values);*
  - *procedure (anche software) di cancellazione selettiva e sicura dei dati a fine ciclo di vita;*
  - *mantenimento dei soli dati legati ad altri obblighi di legge;*
  - *documentazione esplicativa delle soluzioni attuate.*

Per i trasferimenti a (sub-)responsabili del trattamento, descrivere anche le misure tecniche e organizzative specifiche che il (sub-sub) responsabile del trattamento deve attuare per essere in grado di fornire assistenza al titolare e al responsabile (committente) del trattamento.

Descrizione delle misure tecniche e organizzative specifiche che il sub-sub-responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare (e al responsabile committente) del trattamento.

Le stesse misure di sicurezza applicate al sub-responsabile vanno estese a tutta la catena produttiva. Il primo sub-responsabile mantiene la totale responsabilità per tutti i sub-sub responsabili che ha scelto e che ha l'obbligo di comunicare al committente.

NOTE GENERALI

In caso di RTI le misure possono essere ripartite fra i vari soggetti in base alle caratteristiche del trattamento delegato a ciascuna parte. L'obbligazione viene assunta da RTI nella sua interezza e ripartita con documenti interni che devono essere portati all'attenzione del referente del progetto.

Il sub-responsabile è delegato per le attività di gestione e manutenzione dei sistemi informatici e degli applicativi dando piena trasparenza nell'operato a LAZIOcrea ed adegua le sue misure alle misure in essere sui siti produttivi di LAZIOcrea.

La documentazione afferente la certificazione ISO/IEC 27001 è disponibile e scaricabile al seguente link: https://intranet.laziocrea.it/sgsi-isoiec-27001/ tale documentazione sarà resa disponibile ai fornitori da parte dei team di progetto secondo le modalità indicate dagli uffici competenti (e.g. documentazione di gara, documentazione contrattuale, avvio del progetto, ecc..)

ALLEGATO IV

Elenco dei sub-responsabili del trattamento

In caso di RTI tutti i mandanti sono automaticamente individuati quali sub-responsabili della MANDATARIA. E' tuttavia necessario specificare per ciascuno il subtrattamento delegato e l'eventuale posizione dei dati.
In questa tabella è necessario inserire, a titolo informativo, tutti i sub-sub-responsabili funzionali che per qualche motivo gestiscono dati personali sotto la responsabilità del committente.

In caso di trattamenti extra EU indicare sempre la tutela giuridica adottata per il trasferimento al di fuori del SEE.

SUB-TRATTAMENTO DELEGATO	RAGIONE SOCIALE E PIVA DEL SUB-SUB-RESPONSABILE	DATI DI CONTATTO DEL SUB-SUB-RESPONSABILE	POSIZIONE