

REGIONE DEL VENETO



ULSS7
PEDEMONTANA

Via dei Lotti, n. 40
36061 Bassano del Grappa (VI)
Codice fiscale e partita IVA 00913430245

N. 1248 DEL 29/07/2026

DELIBERAZIONE
del

DIRETTORE GENERALE

Nominato con D.P.G.R. n. 21 del 28/02/2026

Coadiuvato dai sigg.:

DIRETTORE AMMINISTRATIVO

dott.ssa LAURA ESPOSITO

DIRETTORE SANITARIO

dr. ANTONIO DI CAPRIO

DIRETTORE DEI SERVIZI SOCIO – SANITARI

dott.ssa PAOLA VESCOVI

OGGETTO: APPROVAZIONE DELLA VERSIONE AGGIORNATA INTEGRATIVA E RETTIFICATIVA DELL' "ACCORDO PER LA NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679" TRA L'AZIENDA ULSS N. 7 PEDEMONTANA E AZIENDA ZERO PER LA GESTIONE DEL SISTEMA INFORMATICO ECM.

IL DIRETTORE GENERALE
DELL'AZIENDA ULSS 7 PEDEMONTANA
dott. Giovanni Carretta

Documento informatico firmato digitalmente ai sensi del D. Lgs n. 82/2005, del T.U. n. 445/2000 e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa; il documento informatico è conservato digitalmente negli archivi informatici dell'Azienda.

Proponente: UOSD FORMAZIONE
Anno Proposta: 2026 Numero Proposta: 1322/26

Il Responsabile dell'U.O.S.D. Formazione, nonché Responsabile del procedimento, attesta che la presente proposta di deliberazione è stata regolarmente istruita nel rispetto della vigente normativa nazionale, regionale e regolamentare: per il Dirigente f.to Michela Piccinini.

Il Responsabile dell'U.O.S.D. Formazione riferisce quanto segue.

Premesso che:

- con deliberazione del Direttore Generale n. 1178 del 10 luglio 2026 è stato approvato lo schema di "Accordo per la nomina a Responsabile del Trattamento dei Dati Personali ai sensi dell'art. 28 del Regolamento UE 2016/679" tra l'Azienda ULSS n. 7 Pedemontana e Azienda Zero per la gestione del sistema informatico ECM;
- in data successiva, a seguito dell'incontro di coordinamento tra i Referenti degli Uffici Privacy delle Aziende Sanitarie della Regione del Veneto ed Azienda Zero, è emersa la necessità di procedere ad una revisione del testo dell'accordo.

Dato atto che:

- in data 24 luglio 2026 l'Ufficio Privacy aziendale ha trasmesso via mail la versione aggiornata, integrativa e rettificativa dell'Accordo per la nomina a Responsabile del Trattamento, precisando che essa annulla e sostituisce integralmente il testo precedentemente approvato con la deliberazione n. 1178/2026, succitata;
- le principali modifiche apportate all'accordo riguardano nello specifico:
 - Perimetro della Titolarità e Ruoli Privacy: esplicitazione dettagliata del ruolo dell'Azienda ULSS 7 in qualità di Provider Pubblico e datore di lavoro, con inserimento della "Matrice essenziale dei ruoli" per delimitare le attività svolte in delega rispetto alle autonome funzioni istituzionali di Azienda Zero e della Regione;
 - Categorie di Interessati e Dati Trattati: dettaglio analitico delle categorie di soggetti coinvolti (Allegato A), disciplina specifica dell'origine dei dati e delle eventuali "categorie particolari di dati";
 - Intelligenza Artificiale (AI) e Profilazione: introduzione del divieto espresso per il Responsabile di impiegare i dati personali per addestrare, validare o alimentare sistemi di AI/modelli algoritmici o per finalità di profilazione;
 - Gestione dei Data Breach: conferma del termine di notifica entro 24 ore (a prescindere dalla valutazione preliminare del rischio) e divieto per il Responsabile di effettuare segnalazioni al Garante o agli interessati in sostituzione del Titolare;
 - Sub-responsabili del Trattamento: delimitazione puntuale e restrittiva dell'ambito operativo dei sub-fornitori (NBS S.r.l. e Fastweb S.p.A.) tramite l'Allegato C;
 - Misure Tecniche e Organizzative: introduzione dell'Allegato B ("Misure minime vincolanti") articolato su 14 aree di sicurezza informatica, inclusa la separazione logica delle banche dati aziendali.

Considerato che il presente provvedimento non comporta alcun impegno di spesa a carico dell'Azienda ULSS 7 Pedemontana.

Per quanto sopra esposto, il Responsabile dell'U.O.S.D. Formazione propone di approvare la versione aggiornata integrativa e rettificativa dell'Accordo con Azienda Zero per la nomina a Responsabile del Trattamento dei dati personali, ai sensi dell'art. 28 del Regolamento UE 2016/679, diretta a disciplinare le procedure e le attività inerenti alla gestione del sistema informatico ECM degli eventi formativi, allegata alla presente deliberazione quale parte integrante e sostanziale.

IL DIRETTORE GENERALE

Vista la relazione e la proposta del Responsabile del procedimento;

Dato atto che il Responsabile del servizio competente ha attestato l'avvenuta regolare istruttoria della pratica, in ordine alla compatibilità con la vigente legislazione statale, regionale e regolamentare;

Acquisito il parere favorevole dei Direttori Amministrativo, Sanitario e dei Servizi Socio-Sanitari, per quanto di rispettiva competenza.

DELIBERA

1. di approvare, per le motivazioni citate in premessa, lo schema aggiornato dell'“Accordo per la nomina a Responsabile del Trattamento dei Dati Personali ai sensi dell'art. 28 del Regolamento UE 2016/679” tra l'Azienda ULSS n. 7 Pedemontana ed Azienda Zero per la gestione della piattaforma informatica ECM, comprensivo dei relativi allegati;
2. di dare atto che la nuova versione dell'accordo annulla e sostituisce integralmente quella approvata con deliberazione n. 1178 del 10/07/2026, citata in premessa;
3. di confermare in ogni sua altra parte quanto stabilito con la deliberazione n. 1178 del 10/07/2026;
4. di dare atto che la presente deliberazione non comporta alcun impegno di spesa a carico del bilancio dell'Azienda ULSS 7 Pedemontana;
5. di dare atto che la presente deliberazione viene pubblicata all'albo del sito istituzionale dell'Azienda per 10 giorni continuativi, inviata contestualmente al Collegio Sindacale e diventa esecutiva il giorno stesso della sua pubblicazione, come da norma regolamentare approvata con deliberazione n. 1386 del 22.07.2022.

ACCORDO PER LA NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL REGOLAMENTO (UE) 2016/679

Azienda ULSS n. 7 Pedemontana (C.F./P.IVA 00913430245), con sede legale in Via dei Lotti, 40 - 36061 Bassano del Grappa (VI), in persona del Direttore Generale pro tempore, in qualità di Titolare del trattamento ai sensi del Regolamento (UE) 2016/679 (di seguito "Titolare" o "Azienda")

e

Azienda per il governo della sanità della Regione del Veneto - Azienda Zero (C.F./P.IVA 05018720283), con sede legale in Passaggio Luigi Gaudenzio, 1 - 35131 Padova, in persona del Direttore Generale pro tempore, in qualità di Responsabile del trattamento ai sensi del Regolamento (UE) 2016/679 (di seguito "Responsabile" o "Azienda Zero")

Premesso che

- gli articoli 16-bis e seguenti del decreto legislativo 30 dicembre 1992, n. 502, disciplinano la formazione continua in ambito sanitario;
- l'art. 2, comma 1, lettera g), n. 4), della legge regionale del Veneto 25 ottobre 2016, n. 19, attribuisce ad Azienda Zero la gestione di attività tecnico-specialistiche per il sistema e per gli enti del Servizio sanitario regionale, comprese le procedure di accreditamento ECM;
- con deliberazione del Direttore Generale di Azienda Zero n. 558 del 5 settembre 2024 è stata indetta la procedura per l'affidamento del servizio di sviluppo del sistema informatico destinato alla gestione dell'accREDITamento dei provider, degli eventi formativi e del monitoraggio della formazione continua in sanità;
- con deliberazione del Direttore Generale di Azienda Zero n. 786 del 2 dicembre 2024 il predetto servizio è stato aggiudicato a NBS S.r.l.;
- l'Azienda, in qualità di provider pubblico e datore di lavoro, determina le finalità e i mezzi essenziali dei trattamenti connessi alla gestione dei propri eventi formativi ECM e non ECM, delle anagrafiche dei propri dipendenti e collaboratori e dei relativi dossier formativi;
- per tali attività l'Azienda intende avvalersi della Piattaforma regionale ECM messa a disposizione da Azienda Zero;
- Azienda Zero effettua, limitatamente alle attività individuate nel presente Accordo e nell'Allegato A, operazioni di trattamento per conto e su istruzione documentata dell'Azienda e deve pertanto essere designata Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679;
- restano estranei alla presente nomina i trattamenti svolti da Azienda Zero, dalla Regione del Veneto o da altri soggetti per autonome finalità istituzionali, di accreditamento, vigilanza, controllo, monitoraggio o adempimento di obblighi normativi, rispetto ai quali i ruoli in materia di protezione dei dati sono determinati dalla normativa applicabile e dagli atti organizzativi pertinenti;
- il presente Accordo è adottato in conformità al Regolamento (UE) 2016/679, al decreto legislativo 30 giugno 2003, n. 196, come modificato, e, per quanto applicabile, alla normativa in materia di sicurezza informatica, incluso il decreto legislativo 4 settembre 2024, n. 138, di attuazione della direttiva (UE) 2022/2555;
- le Parti intendono disciplinare in modo puntuale i trattamenti effettuati dal Responsabile per conto del Titolare, conformemente all'art. 28, paragrafo 3, del Regolamento (UE) 2016/679.

Tutto ciò premesso, le Parti convengono e stipulano quanto segue.

1. Premesse, allegati e definizioni

Le premesse e gli Allegati A, B, C e D costituiscono parte integrante e sostanziale del presente Accordo.

I termini "dato personale", "trattamento", "interessato", "titolare del trattamento", "responsabile del trattamento", "violazione dei dati personali" e "autorità di controllo" hanno il significato attribuito loro dal Regolamento (UE) 2016/679 (di seguito "GDPR").

Per "Piattaforma" si intende il sistema informatico regionale per la gestione dell'accREDITamento dei provider, degli eventi formativi e del monitoraggio della formazione continua in sanità, limitatamente alle funzionalità utilizzate dall'Azienda nell'ambito dei trattamenti descritti nell'Allegato A.

Per "Ulteriore Responsabile" si intende il soggetto al quale Azienda Zero affida, previa autorizzazione del Titolare, specifiche attività di trattamento necessarie all'erogazione dei servizi oggetto del presente Accordo.

2. Nomina e oggetto

L'Azienda nomina Azienda Zero Responsabile del trattamento ai sensi dell'art. 28 del GDPR esclusivamente per le operazioni descritte nel presente Accordo e nell'Allegato A. Azienda Zero accetta la nomina e si impegna a trattare i dati personali per conto del Titolare nel rispetto delle istruzioni documentate ricevute.

La nomina non comprende né modifica la qualificazione dei trattamenti svolti da Azienda Zero, dalla Regione del Veneto o da altri soggetti per finalità autonome o in adempimento di compiti istituzionali propri. Tali trattamenti restano fuori dal perimetro del presente Accordo.

Azienda Zero dichiara di possedere esperienza, capacità, affidabilità e risorse organizzative e tecniche adeguate a garantire che i trattamenti soddisfino i requisiti del GDPR e tutelino i diritti e le libertà degli interessati. Ogni mutamento rilevante di tali condizioni è comunicato senza ingiustificato ritardo al Titolare.

3. Istruzioni, finalità e limiti del trattamento

Il Responsabile tratta i dati personali soltanto su istruzione documentata del Titolare, risultante dal presente Accordo, dai relativi Allegati e dalle ulteriori comunicazioni scritte impartite dai soggetti autorizzati dall'Azienda.

Il Responsabile non utilizza i dati personali per finalità proprie, ulteriori o incompatibili, non li combina con dati trattati per conto di altri titolari e non li impiega per attività commerciali, profilazione, sviluppo di prodotti o analisi non richieste dal Titolare.

Salvo preventiva autorizzazione scritta del Titolare e specifico aggiornamento dell'Allegato A, il Responsabile non utilizza i dati personali per addestrare, validare, testare o alimentare sistemi di intelligenza artificiale o modelli algoritmici destinati a finalità diverse dall'esecuzione delle istruzioni del Titolare.

Qualora il Responsabile ritenga che un'istruzione violi il GDPR o altra disposizione applicabile in materia di protezione dei dati, ne informa immediatamente il Titolare e sospende, ove necessario, l'esecuzione della sola istruzione contestata fino al ricevimento di indicazioni conformi alla normativa.

Qualora il diritto dell'Unione o nazionale imponga al Responsabile un trattamento non previsto dalle istruzioni del Titolare, il Responsabile informa previamente il Titolare dell'obbligo giuridico, salvo che la legge vieti tale informazione per rilevanti motivi di interesse pubblico.

4. Durata

Il presente Accordo acquista efficacia alla data dell'ultima sottoscrizione e rimane valido per tutta la durata dell'utilizzo della Piattaforma da parte dell'Azienda e, comunque, finché Azienda Zero effettua trattamenti per conto del Titolare.

Gli obblighi che, per loro natura, sono destinati a sopravvivere alla cessazione del rapporto, inclusi riservatezza, restituzione o cancellazione dei dati, cooperazione in caso di violazioni e responsabilità, continuano a produrre effetti anche dopo la cessazione del presente Accordo.

5. Obblighi generali del Responsabile

Nell'esecuzione delle attività affidate, Azienda Zero si impegna a:

- a) rispettare i principi applicabili al trattamento dei dati personali, con particolare riguardo a liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza, protezione dei dati fin dalla progettazione e per impostazione predefinita;
- b) trattare esclusivamente i dati e compiere esclusivamente le operazioni necessarie all'esecuzione delle attività descritte nell'Allegato A;
- c) garantire che le persone autorizzate al trattamento siano vincolate alla riservatezza e ricevano istruzioni adeguate e formazione periodica;
- d) tenere un registro delle categorie di attività di trattamento svolte per conto del Titolare ai sensi dell'art. 30, paragrafo 2, del GDPR;

- e) assistere il Titolare nell'adempimento degli obblighi previsti dagli artt. 32, 33, 34, 35 e 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni disponibili;
- f) assistere il Titolare nella gestione delle richieste degli interessati secondo quanto previsto dall'art. 9 del presente Accordo;
- g) cooperare con il Responsabile della protezione dei dati del Titolare e con le funzioni aziendali competenti;
- h) non comunicare o rendere accessibili i dati a terzi, né diffonderli, salvo istruzione documentata del Titolare o obbligo di legge;
- i) garantire l'esattezza e l'aggiornamento dei dati nei limiti delle operazioni affidate e delle istruzioni ricevute;
- j) mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto del presente Accordo e dell'art. 28 del GDPR;
- k) informare senza ingiustificato ritardo il Titolare di eventi, richieste, modifiche organizzative o tecniche che possano incidere significativamente sulla protezione dei dati o sull'idoneità del Responsabile a svolgere l'incarico.

Salvo i casi di urgenza o i termini più brevi previsti dal presente Accordo, le informazioni e i documenti richiesti dal Titolare sono forniti entro dieci giorni lavorativi dalla richiesta.

6. Persone autorizzate e amministratori di sistema

Il Responsabile individua per iscritto le persone autorizzate a trattare i dati personali, delimita i rispettivi ambiti operativi, impartisce istruzioni documentate e verifica periodicamente la permanenza delle autorizzazioni e la necessità dei relativi privilegi.

Qualora le attività comportino funzioni riconducibili all'amministrazione di sistema, Azienda Zero designa nominativamente gli amministratori di sistema, attribuisce ambiti di operatività specifici e documentati e applica le prescrizioni del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato.

Il Responsabile garantisce credenziali individuali, separazione tra utenze amministrative e ordinarie, autenticazione a più fattori per gli accessi privilegiati, registrazione degli accessi logici degli amministratori e conservazione dei relativi log per almeno sei mesi o per il periodo superiore previsto dalle politiche regionali applicabili.

L'elenco aggiornato degli amministratori di sistema e dei relativi ambiti di operatività è reso disponibile al Titolare su richiesta, con modalità che ne preservino la sicurezza e la riservatezza.

7. Misure tecniche e organizzative di sicurezza

Il Responsabile adotta e mantiene, ai sensi dell'art. 32 del GDPR, misure tecniche e organizzative adeguate al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà degli interessati.

Le misure minime vincolanti sono descritte nell'Allegato B. Il Responsabile integra nell'Allegato B, prima dell'avvio del trattamento o della sottoscrizione del presente Accordo, le informazioni relative alle infrastrutture effettivamente utilizzate, alla localizzazione dei dati e delle copie di sicurezza, ai fornitori cloud, ai livelli di servizio di continuità operativa e alle ulteriori misure applicate.

Il Responsabile non modifica le misure di sicurezza in modo da ridurre il livello di protezione concordato. Le modifiche rilevanti dell'architettura, dei luoghi di trattamento o delle misure sono comunicate preventivamente al Titolare, salvo gli interventi urgenti necessari a fronteggiare vulnerabilità o incidenti, che sono comunicati appena possibile.

Il Responsabile garantisce la separazione logica dei dati riferiti alle diverse Aziende e impedisce che utenti o soggetti operanti per conto di altri titolari possano accedere ai dati dell'Azienda.

8. Violazioni dei dati personali

Il Responsabile informa il Titolare di qualsiasi violazione dei dati personali riguardante dati trattati per conto dell'Azienda, anche se verificatasi presso un Ulteriore Responsabile, senza ingiustificato ritardo e comunque entro ventiquattro ore dal momento in cui ne è venuto a conoscenza, indipendentemente da una preliminare valutazione del rischio per i diritti e le libertà degli interessati.

La comunicazione iniziale contiene tutte le informazioni disponibili e, per quanto possibile:

- una descrizione della natura della violazione, della data e dell'ora di rilevazione e delle circostanze note;
- le categorie e il numero approssimativo di interessati e di registrazioni coinvolte;
- le categorie di dati personali interessate;
- le probabili conseguenze della violazione;
- le misure già adottate o proposte per contenere la violazione e mitigarne gli effetti;
- i recapiti del referente operativo e del Responsabile della protezione dei dati di Azienda Zero;
- ogni elemento utile al Titolare per valutare gli adempimenti previsti dagli artt. 33 e 34 del GDPR.

Le informazioni non ancora disponibili sono trasmesse progressivamente, senza ingiustificato ritardo. Il Responsabile non attende il completamento dell'analisi tecnica prima di effettuare la comunicazione iniziale.

Il Responsabile conserva le evidenze dell'evento, coopera alle attività di analisi e contenimento, attua tempestivamente le misure correttive concordate e fornisce al Titolare gli aggiornamenti richiesti fino alla chiusura dell'incidente.

Il Responsabile non effettua notifiche all'Autorità di controllo né comunicazioni agli interessati per conto del Titolare, salvo espressa istruzione documentata o autonomo obbligo di legge, del quale informa il Titolare nei limiti consentiti.

9. Esercizio dei diritti degli interessati

Tenuto conto della natura del trattamento, il Responsabile assiste il Titolare con misure tecniche e organizzative adeguate per consentire il riscontro alle richieste di esercizio dei diritti previste dagli artt. 12-22 del GDPR.

Qualora riceva direttamente una richiesta riferibile ai trattamenti disciplinati dal presente Accordo, Azienda Zero la trasmette al Titolare senza ingiustificato ritardo e, comunque, entro un giorno lavorativo, utilizzando i recapiti dell'Allegato D. Il Responsabile non fornisce un riscontro autonomo all'interessato, salvo istruzione documentata del Titolare.

Il Responsabile rende disponibili, nei tempi indicati dal Titolare, i dati, i log e le informazioni necessari a verificare l'identità del richiedente, ricostruire i trattamenti e predisporre il riscontro.

10. Valutazione d'impatto e consultazione preventiva

Il Responsabile assiste il Titolare, tenuto conto della natura del trattamento e delle informazioni disponibili, nello svolgimento delle valutazioni d'impatto sulla protezione dei dati e delle eventuali consultazioni preventive dell'Autorità di controllo.

A tale fine, Azienda Zero fornisce informazioni documentate sull'architettura, sui flussi dei dati, sui soggetti coinvolti, sulle misure di sicurezza, sui rischi individuati, sui trasferimenti e sugli Ulteriori Responsabili utilizzati.

11. Informazioni, verifiche e audit

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi previsti dal GDPR e dal presente Accordo, incluse certificazioni, relazioni di audit, esiti di test di sicurezza, sintesi delle verifiche sui fornitori e documentazione delle misure tecniche e organizzative.

Il Titolare può effettuare, direttamente o tramite soggetti indipendenti vincolati alla riservatezza, verifiche documentali e audit sulle attività di trattamento. Le verifiche sono concordate con ragionevole preavviso e condotte in modo da non compromettere la sicurezza o la continuità dei servizi.

Il preavviso non è richiesto quando l'audit sia necessario a seguito di una violazione, di un fondato sospetto di non conformità o di una richiesta dell'Autorità di controllo.

Ciascuna Parte sostiene i propri costi ordinari di verifica. Qualora l'audit accerti una grave non conformità imputabile al Responsabile, Azienda Zero adotta senza ritardo le misure correttive e sostiene i costi direttamente necessari alla loro attuazione.

12. Ulteriori Responsabili del trattamento

Con la sottoscrizione del presente Accordo, il Titolare autorizza specificamente gli Ulteriori Responsabili elencati nell'Allegato C, nei limiti delle attività e delle condizioni ivi descritte.

Per ogni futura aggiunta o sostituzione, il Titolare conferisce ad Azienda Zero un'autorizzazione generale subordinata alla comunicazione preventiva, mediante posta elettronica certificata, di almeno quindici giorni. La comunicazione deve indicare identità, sede, attività affidate, categorie di dati accessibili, luoghi di trattamento, eventuali trasferimenti e misure di sicurezza rilevanti.

Entro il predetto termine il Titolare può opporsi per motivi documentati connessi alla protezione dei dati personali. In caso di opposizione, le Parti cooperano in buona fede per individuare una soluzione conforme; fino alla definizione della questione, il nuovo soggetto non accede ai dati dell'Azienda.

Azienda Zero stipula con ciascun Ulteriore Responsabile un atto scritto che impone obblighi sostanzialmente equivalenti a quelli previsti dal presente Accordo, verifica le garanzie offerte e conserva la relativa documentazione a disposizione del Titolare.

Azienda Zero rimane pienamente responsabile nei confronti del Titolare dell'adempimento degli obblighi affidati agli Ulteriori Responsabili e comunica senza ingiustificato ritardo ogni modifica delle attività o delle condizioni indicate nell'Allegato C.

13. Trasferimenti verso Paesi terzi e servizi cloud

Il Responsabile non trasferisce né consente l'accesso, anche per assistenza, manutenzione, conservazione o amministrazione tecnica, ai dati personali da Paesi situati al di fuori dello Spazio economico europeo o da parte di organizzazioni internazionali senza preventiva autorizzazione scritta del Titolare.

Quando il trasferimento sia autorizzato, il Responsabile assicura il rispetto del Capo V del GDPR mediante una decisione di adeguatezza o, in sua assenza, garanzie adeguate ai sensi dell'art. 46 del GDPR. Se sono utilizzate clausole contrattuali standard, il Responsabile svolge e documenta la valutazione dell'impatto del trasferimento e adotta le misure supplementari necessarie a garantire un livello di protezione sostanzialmente equivalente a quello dell'Unione europea.

Il Responsabile dichiara nell'Allegato B e nell'Allegato C i fornitori cloud, i luoghi di conservazione primaria e di backup, i Paesi dai quali può avvenire l'accesso e gli eventuali ulteriori soggetti della catena di fornitura.

Il Responsabile informa tempestivamente il Titolare di richieste di accesso ai dati formulate da autorità pubbliche di Paesi terzi, salvo divieti di legge, e adotta le iniziative ragionevolmente necessarie per contestare le richieste che ritenga illegittime o sproporzionate.

14. Conservazione, restituzione e cancellazione

Il Responsabile conserva i dati personali soltanto per il periodo necessario all'esecuzione delle istruzioni del Titolare e secondo i criteri indicati nell'Allegato A o nelle successive istruzioni documentate.

Alla cessazione del rapporto, per qualsiasi causa, il Responsabile, su scelta del Titolare, restituisce i dati personali in formato strutturato e interoperabile oppure li cancella definitivamente, incluse le copie, salvo che il diritto dell'Unione o nazionale ne imponga la conservazione.

Le copie presenti nei sistemi di backup sono rese indisponibili all'uso ordinario e cancellate secondo il ciclo tecnico di sovrascrittura documentato nell'Allegato B. Fino alla cancellazione definitiva, esse restano protette e non possono essere ripristinate salvo necessità di continuità operativa o obbligo di legge.

Il Responsabile rilascia al Titolare un'attestazione scritta dell'avvenuta restituzione o cancellazione e indica le eventuali informazioni conservate per obbligo di legge, la relativa base giuridica e il periodo di conservazione.

15. Ispezioni e richieste delle Autorità

Il Responsabile informa tempestivamente il Titolare di ispezioni, richieste di informazioni o ordini dell'Autorità di controllo o di altre autorità competenti riguardanti i trattamenti svolti per conto dell'Azienda, salvo che un obbligo di legge vieti tale comunicazione.

Azienda Zero assiste il Titolare nella predisposizione dei riscontri e coopera durante le verifiche, mettendo a disposizione le informazioni e la documentazione pertinenti.

16. Responsabilità

Le Parti rispondono delle violazioni e dei danni secondo la ripartizione prevista dalla normativa applicabile, inclusi gli artt. 28 e 82 del GDPR.

Il Responsabile risponde dei trattamenti effettuati in violazione degli obblighi specificamente diretti ai responsabili dal GDPR o in difformità dalle legittime istruzioni del Titolare, nei limiti previsti dalla normativa applicabile.

Qualora Azienda Zero determini, in violazione del GDPR, le finalità e i mezzi di uno specifico trattamento, è considerata titolare con riferimento a tale trattamento ai sensi dell'art. 28, paragrafo 10, del GDPR, ferme restando le ulteriori responsabilità previste dalla legge.

Il Responsabile comunica prontamente al Titolare le situazioni sopravvenute che possano incidere sulla propria idoneità a svolgere l'incarico o sulla conformità dei trattamenti.

17. Prevalenza, comunicazioni e modifiche

Per le materie relative alla protezione dei dati personali, il presente Accordo prevale sulle disposizioni incompatibili contenute in contratti, convenzioni o altri atti collegati, fatti salvi gli obblighi inderogabili di legge.

Le comunicazioni formali previste dal presente Accordo sono effettuate ai recapiti indicati nell'Allegato D. La modifica dei soli recapiti o dei nominativi operativi può essere comunicata mediante posta elettronica certificata senza necessità di nuova sottoscrizione.

Ogni modifica sostanziale dell'oggetto, delle finalità, delle categorie di dati, delle categorie di interessati, delle operazioni, delle misure di sicurezza, dei trasferimenti o degli obblighi delle Parti deve essere concordata per iscritto e sottoscritta da entrambe le Parti.

18. Disposizioni finali

L'obbligo di riservatezza resta efficace anche dopo la scadenza o la cessazione del presente Accordo.

L'eventuale nullità o inefficacia di una disposizione non pregiudica la validità delle restanti clausole. Le Parti sostituiscono la disposizione invalida con una previsione conforme alla legge e quanto più possibile equivalente nella funzione.

Il presente Accordo è sottoscritto digitalmente. Il regime dell'imposta di bollo e della registrazione è applicato, ove dovuto, secondo la normativa vigente e le indicazioni degli uffici competenti.

Data _____

Per l'Azienda ULSS n. 7 Pedemontana
Il Direttore Generale

Data _____

Per Azienda Zero
Il Direttore Generale

ALLEGATO A

DESCRIZIONE DEL TRATTAMENTO E ISTRUZIONI DEL TITOLARE

Elemento	Descrizione e istruzioni
Oggetto del trattamento	Messa a disposizione, gestione tecnica e operativa, manutenzione e assistenza della Piattaforma, limitatamente alle funzionalità utilizzate dall'Azienda per la gestione dei propri eventi formativi ECM e non ECM, delle anagrafiche degli utenti e dei dossier formativi.
Durata	Dalla data di efficacia del presente Accordo fino alla cessazione dell'utilizzo della Piattaforma e al completamento delle attività di restituzione o cancellazione previste dall'art. 14.
Finalità determinate dal Titolare	Gestione delle attività formative organizzate o gestite dall'Azienda; amministrazione delle anagrafiche dei dipendenti, collaboratori e utenti esterni; gestione di iscrizioni, presenze, valutazioni, attestazioni e crediti; gestione dei dossier formativi individuali e di gruppo; gestione dell'albo dei docenti e delle figure coinvolte negli eventi; produzione di reportistica aziendale.
Natura e operazioni	Raccolta e importazione; registrazione; organizzazione e strutturazione; consultazione; abilitazione e gestione dei profili; modifica e aggiornamento; elaborazione; estrazione; generazione di attestazioni e report; comunicazione ai destinatari indicati dal Titolare o previsti dalla normativa; conservazione; limitazione; restituzione; cancellazione.
Modalità	Trattamento con strumenti informatici e telematici attraverso la Piattaforma e i sistemi tecnici strettamente connessi alla sua erogazione.
Categorie di dati personali	Dati identificativi e di contatto; codice fiscale e identificativi della Piattaforma; ente, struttura e unità organizzativa di appartenenza; rapporto di lavoro o collaborazione; qualifica, professione, disciplina, ruolo e, ove pertinente, iscrizione a ordini o albi; dati relativi a iscrizione, partecipazione, presenza, frequenza, valutazione, completamento e crediti formativi; dati dei dossier formativi individuali e di gruppo; dati relativi a docenti, relatori, moderatori, tutor, responsabili scientifici, coordinatori ed esperti; credenziali, profili autorizzativi, log di accesso e dati tecnici di utilizzo.
Categorie particolari di dati	La Piattaforma non è destinata ordinariamente alla raccolta di categorie particolari di dati ai sensi dell'art. 9 GDPR. L'eventuale trattamento di informazioni relative a disabilità, esigenze sanitarie o accomodamenti per la partecipazione agli eventi può essere avviato soltanto su specifica istruzione documentata del Titolare, previa verifica della base giuridica, della necessità, delle misure di sicurezza e aggiornamento del presente Allegato.
Categorie di interessati	Dipendenti e collaboratori dell'Azienda; utenti esterni iscritti agli eventi; personale dell'Azienda con ruoli nel provider; docenti, relatori, moderatori, tutor, responsabili scientifici, coordinatori ed esperti di contenuto; utenti autorizzati alla gestione della Piattaforma.
Origine dei dati	Sistemi di gestione delle risorse umane dell'Azienda; inserimento diretto da parte dell'Azienda o degli utenti autorizzati; dati prodotti nel corso della gestione e della fruizione degli eventi formativi.

Elemento	Descrizione e istruzioni
Destinatari	Persone autorizzate dal Titolare e dal Responsabile nei limiti delle rispettive funzioni; Ulteriori Responsabili autorizzati; soggetti ai quali la comunicazione sia disposta dal Titolare o prevista dalla normativa ECM applicabile. Le comunicazioni effettuate da Azienda Zero o dalla Regione per autonome finalità istituzionali restano escluse dalla presente nomina.
Conservazione	Per i periodi definiti dal Titolare nelle proprie istruzioni e nel piano di conservazione applicabile alle attività formative, nonché per gli eventuali termini imposti dalla normativa ECM. Azienda Zero non determina autonomamente i tempi di conservazione e mette a disposizione le funzionalità necessarie alla cancellazione, limitazione, esportazione e restituzione.
Decisioni automatizzate e IA	Nessuna decisione automatizzata con effetti giuridici o analogamente significativi e nessun utilizzo dei dati per addestrare o testare sistemi di intelligenza artificiale, salvo preventiva istruzione scritta del Titolare e aggiornamento del presente Accordo.

Matrice essenziale dei ruoli

Attività	Titolare / qualificazione	Responsabile / qualificazione
Gestione degli eventi formativi organizzati o amministrati dall'Azienda, delle anagrafiche aziendali e dei dossier formativi	Azienda ULSS n. 7 Pedemontana	Azienda Zero, nei limiti del presente Accordo
Accreditamento dei provider, vigilanza, controllo e monitoraggio svolti per finalità istituzionali regionali o proprie	Fuori dal perimetro del presente Accordo; il ruolo è determinato dalla normativa e dagli atti organizzativi applicabili	Fuori dal perimetro del presente Accordo
Attività affidate ai soggetti elencati nell'Allegato C	Azienda ULSS n. 7 Pedemontana	Azienda Zero quale Responsabile; fornitori quali Ulteriori Responsabili nei limiti autorizzati

ALLEGATO B

MISURE TECNICHE E ORGANIZZATIVE

Le misure indicate nel presente Allegato costituiscono requisiti minimi vincolanti. Azienda Zero mantiene una descrizione tecnica aggiornata della loro attuazione e la rende disponibile al Titolare su richiesta.

Area	Misure minime
Governance e responsabilità	Politiche documentate in materia di sicurezza e protezione dei dati; attribuzione di ruoli e responsabilità; riesame periodico dei rischi; formazione iniziale e periodica del personale; gestione documentata delle eccezioni.
Controllo degli accessi	Credenziali individuali; principio del minimo privilegio e necessità di conoscere; processi di provisioning, modifica e revoca; revisione periodica dei profili; blocco degli account inattivi; autenticazione a più fattori per accessi privilegiati e remoti.
Amministrazione di sistema	Designazione nominativa; ambiti operativi specifici; utenze amministrative separate; registrazione degli accessi e delle attività rilevanti; protezione dei log da alterazioni; conservazione per almeno sei mesi o per il maggior periodo previsto dalle politiche applicabili.
Cifratura e comunicazioni	Cifratura dei dati in transito mediante protocolli aggiornati e sicuri; cifratura a riposo quando appropriata rispetto al rischio; gestione protetta delle chiavi e separazione delle responsabilità; divieto di trasmissione mediante canali non autorizzati.
Separazione dei dati	Separazione logica dei dati delle diverse Aziende e degli ambienti di sviluppo, test e produzione; utilizzo di dati sintetici o anonimizzati negli ambienti non produttivi, salvo necessità documentata e applicazione di misure equivalenti.
Logging e monitoraggio	Registrazione degli accessi, delle operazioni amministrative e degli eventi di sicurezza; sincronizzazione temporale; monitoraggio degli eventi anomali; procedure di escalation; accesso ai log limitato e tracciato.
Backup, continuità e ripristino	Backup periodici, protetti e separati; test di ripristino; piani di continuità operativa e disaster recovery; definizione e comunicazione di RPO e RTO; verifica almeno annuale dei piani e dopo modifiche rilevanti.
Gestione delle vulnerabilità	Inventario degli asset; gestione delle configurazioni; scansioni periodiche; aggiornamento e patching secondo la criticità; test di sicurezza e penetration test periodici; tracciamento e chiusura delle azioni correttive.
Sviluppo e cambiamenti	Principi di sicurezza e protezione dei dati fin dalla progettazione; revisione del codice e delle configurazioni; segregazione dei compiti; test prima del rilascio; gestione documentata delle modifiche e possibilità di rollback.
Protezione da codice malevolo e attacchi	Misure antimalware ed endpoint protection; filtraggio e protezione perimetrale; sistemi di rilevazione e prevenzione; protezione da attacchi di saturazione ove pertinente; aggiornamento delle firme e delle regole di rilevazione.
Gestione degli incidenti	Procedura formalizzata di rilevazione, contenimento, analisi, conservazione delle evidenze, comunicazione e chiusura; reperibilità dei referenti; esercitazioni periodiche; rispetto del termine di comunicazione di cui all'art. 8.
Sicurezza fisica	Controlli di accesso ai locali e ai data center; registrazione degli accessi; protezione ambientale; continuità dell'alimentazione; misure antincendio e di protezione delle apparecchiature.



Area	Misure minime
Cancellazione e dismissione	Procedure di cancellazione sicura e verificabile; sanificazione o distruzione dei supporti; gestione delle copie di backup; attestazione della cancellazione o restituzione alla cessazione del rapporto.
Gestione dei fornitori	Valutazione preventiva e periodica delle garanzie; accordi conformi all'art. 28 GDPR; controllo della catena di subfornitura; obblighi in materia di sicurezza, incidenti, cancellazione, audit e trasferimenti.
Verifica dell'efficacia	Audit, controlli e test periodici dell'efficacia delle misure; conservazione delle evidenze; riesame dopo incidenti, modifiche rilevanti o variazioni del rischio.

ALLEGATO C

ULTERIORI RESPONSABILI AUTORIZZATI

L'autorizzazione è limitata alle attività riportate nella tabella e presuppone che Azienda Zero completi, prima dell'accesso ai dati dell'Azienda, le informazioni tecniche e organizzative richieste nel presente Allegato.

Ragione sociale	Sede legale	Contatto	Attività autorizzata
NBS S.r.l.	Via Val Tiberina, 23/A - San Benedetto del Tronto (AP)	nbspec@pec.it	Attività connesse al servizio di sviluppo del sistema informatico aggiudicato con deliberazione di Azienda Zero n. 786/2024 e supporto alla gestione dei corsi ECM e non ECM, nei limiti in cui tali attività comportino trattamento di dati per conto dell'Azienda.
Fastweb S.p.A.	Piazza Adriano Olivetti, 1 - Milano (MI)	fastweb@pec.fastweb.it	Manutenzione, assistenza e supporto sistemistico limitatamente alle componenti ICT utilizzate per l'erogazione della Piattaforma ECM e nei limiti in cui tali attività comportino trattamento di dati per conto dell'Azienda.

Per ciascun Ulteriore Responsabile Azienda Zero conserva e rende disponibili al Titolare:

- il contratto o altro atto giuridico conforme all'art. 28, paragrafi 3 e 4, del GDPR;
- la valutazione delle garanzie tecniche e organizzative offerte;
- la descrizione delle operazioni, dei dati accessibili, dei luoghi di trattamento e degli eventuali ulteriori soggetti della catena di fornitura;
- le informazioni relative a eventuali trasferimenti o accessi da Paesi terzi;
- le procedure di comunicazione degli incidenti e di restituzione o cancellazione dei dati.