

Contratto tra titolare e responsabile del trattamento dei dati per il software No-Q

tra:

si prega di compilare

e

No-Q srl, via Brennero 32, 39042 Bressanone (IT), telefono: +39 0472 611753
e-mail: office@no-q.info, e-mail responsabile della protezione dei dati: dpo@no-q.info

Il presente Contratto è parte integrante del Contratto principale tra No-Q srl (di seguito denominata "Fornitore") e il Cliente (di seguito "Committente"; insieme le "Parti") relativo alla fornitura del software No-Q (di seguito: "Contratto di base").

1. Introduzione, campo di applicazione, definizioni

1.1 Le presenti disposizioni sul trattamento disciplinano i diritti e gli obblighi del Committente e del Fornitore in relazione al trattamento dei dati personali ai sensi e per gli effetti di cui all'articolo 28, paragrafo 3, del regolamento (UE) 2016/679 (di seguito: RGPD).

1.2 Il presente Contratto si applica a tutte le attività in cui il Fornitore, i suoi collaboratori o i subappaltatori da esso incaricati (Subfornitori) trattano dati personali per conto del Committente nell'ambito del Contratto di base.

1.3 I termini utilizzati in queste disposizioni sul trattamento dei dati sono da intendersi secondo la definizione che ne viene data nel RGPD.

1.4. Se non espressamente definito diversamente, il Committente è considerato il "Titolare del trattamento" ai sensi dell'articolo 4 n. 7 del RGPD e il Fornitore è considerato il "Responsabile del trattamento" ai sensi dell'articolo 4 n. 8 del RGPD.

2. Oggetto e durata del trattamento

2.1 Oggetto. Il Fornitore gestisce i seguenti tipi di trattamento: trattamento di dati per l'esecuzione del servizio No-Q come descritto nel Contratto di base (di seguito anche "Sistema No-Q").

2.2 Durata. Il presente Contratto è valido per tutta la durata del Contratto principale.

3. Natura e finalità della raccolta, del trattamento o dell'utilizzo dei dati

3.1 Natura e finalità del trattamento: visualizzare su richiesta, salvare, modificare su richiesta, trasmettere su richiesta, anonimizzare secondo le specifiche del cliente.

- Esecuzione del servizio No-Q (incl. supporto tecnico)
- Generazione di un QR code leggibile (es. per il portale Abda)
- Ordinazione, stampa e spedizione dell'Immune-ID
- Erogazione del servizio di prescrizione elettronica (scansione della ricetta da parte del cliente e trasmissione alla farmacia)
- Altri servizi forniti da No-Q su richiesta del cliente

3.2 Natura dei dati: Salvo quanto espresso al punto 3.3, il trattamento da parte del Fornitore può includere le seguenti categorie di dati personali, a seconda della configurazione del Sistema No-Q da parte del Committente:

Dati dei collaboratori del Committente:

- Nome
- Cognome
- Indirizzo e-mail
- Data di nascita
- Indirizzo
- Città
- Codice postale
- Telefono
- Cellulare
- Log-Files
- IBAN/BIC
- Assicurazione sanitaria
- Codice fiscale

Dati dei clienti del Committente:

- Nome
- Cognome
- Indirizzo e-mail
- Indirizzo
- Città
- Codice postale
- Nazionalità
- Paese (di residenza)
- Telefono
- Cellulare
- Data di nascita
- Codice fiscale
- Indirizzo IP
- Informazioni sulla carta di credito
- Stato di appartenenza come membro
- Numero di passaporto/carta d'identità
- Dettagli della prenotazione effettuata: ID della prenotazione, ora della

registrazione

- Dati del test COVID-19 effettuato: data del test, luogo del test, analisi, medico, servizio, test, kit di test, tipo di test, esito del test (risultato)
- Informazioni aggiuntive sul test COVID-19 effettuato in caso di utilizzo di un dispositivo di lettura automatica KLS: foto del kit di test
- Dettagli della vaccinazione: data della vaccinazione, tipo di vaccinazione, vaccino, servizio (produttore), numero di lotto, patologie croniche preesistenti, medico, indicazioni sulla seconda dose
- Informazioni per la digitalizzazione del certificato di vaccinazione: vaccino/i ricevuto/i, data/e di vaccinazione, certificazione di vaccinazione digitale
- Dati dei clienti che ordinano Immune-ID: Nome, indirizzo, certificato COVID digitale dell'UE (e informazioni in esso contenute)
- Dati aggiuntivi per la prescrizione elettronica: foto della ricetta comprensiva di contenuto (azienda di assicurazione sanitaria, indirizzo di residenza, data, n. assicurazione sanitaria, n. assicurato, stato, n. azienda, n. medico, farmaci prescritti e assunzione, giorno dell'infortunio in caso di infortunio sul lavoro e numero del datore di lavoro, timbro del medico a contratto e firma del medico, informazioni sul costo dei farmaci, informazioni sul ritiro dei farmaci, informazioni sulla consegna, compreso l'indirizzo, se del caso)
- Dati aggiuntivi per l'elaborazione di altri servizi farmaceutici: Data e ora dell'appuntamento prenotato, ulteriori informazioni determinate individualmente

Categorie di persone interessate dal trattamento:

- collaboratori del Committente
- clienti del Committente
- medici

3.3 Trattamento di categorie particolari di dati personali (art. 9): il Fornitore può avere accesso alle informazioni sanitarie degli interessati per finalità di supporto. In linea di principio il trattamento dei dati relativi alla salute è limitato alla fornitura del sistema.

3.4 Il Committente assicura e garantisce di aver rispettato e di continuare a rispettare tutte le leggi applicabili, comprese le leggi sulla protezione dei dati, in merito al trattamento dei dati e a tutte le istruzioni sul trattamento che darà al Fornitore, assicura e garantisce altresì di aver fornito e di continuare a fornire tutte le comunicazioni e di aver ricevuto e di continuare a ricevere tutti i consensi e diritti necessari ai sensi delle leggi sulla protezione dei dati per il trattamento dei dati personali da parte del Fornitore per le finalità descritte nel Contratto. Il Committente è l'unico responsabile dell'esattezza, della qualità e della liceità dei dati personali trasmessi al Fornitore per il trattamento e dei mezzi con cui ha acquisito i dati. Fatto salvo il carattere generale di quanto sopra, il Committente conviene di essere responsabile del rispetto di tutte le leggi (comprese le leggi sulla protezione dei dati).

3.5 Il Committente garantisce che il trattamento dei dati da parte del Fornitore in conformità con le istruzioni del Committente non comporterà la violazione da parte del Fornitore di leggi, regolamenti o norme applicabili, comprese, ma non solo, le leggi sulla protezione dei dati.

3.6 Il contraente è autorizzato a realizzare valutazioni statistiche anonime. Questo ha lo scopo di identificare le tendenze, sulla base delle quali, per esempio, i servizi possono essere adattati. Tali valutazioni statistiche e anonime possono anche essere messe a disposizione delle autorità. Un'eventuale pubblicazione dei dati anonimizzati è consentita e avviene esclusivamente in forma aggregata (ad esempio: tasso di positività per stato federale, per gruppo di età).

4. Obblighi del Fornitore

4.1 Il Fornitore tratta i dati personali esclusivamente come concordato contrattualmente o secondo le istruzioni del Committente, salvo che il Fornitore sia obbligato per legge ad effettuare un trattamento specifico. Se è soggetto a tale obbligo, il Fornitore deve informare il Committente prima del trattamento, salvo che la legge vieti tale informazione. Il Fornitore, inoltre, non utilizzerà i dati forniti per il trattamento per altre finalità, in particolare per scopi propri.

4.2 Il Fornitore conferma di essere a conoscenza delle pertinenti norme generali sulla protezione dei dati. Rispetta i principi di un corretto trattamento dei dati.

4.3 Se non espressamente concordato diversamente, il Committente è responsabile del rispetto delle disposizioni che vanno oltre le norme generali sulla protezione dei dati (ad esempio il rispetto di obblighi di conservazione stabiliti in disposizioni speciali).

4.4 Il Fornitore si impegna a mantenere assoluta riservatezza durante il trattamento.

4.5 Eventuali persone che potrebbero venire a conoscenza dei dati trattati nell'ambito dell'incarico si impegnano in forma scritta a mantenere la riservatezza, qualora non siano già soggette per legge a un obbligo di segretezza pertinente.

4.6 Il Fornitore assicura che le persone da lui impiegate per il trattamento sono state rese edotte delle disposizioni pertinenti sulla protezione dei dati e del presente Contratto prima dell'inizio del trattamento. Eventuali misure di formazione e di sensibilizzazione in merito devono essere ripetute su base regolare e appropriata. Il Fornitore provvede a istruire e monitorare adeguatamente su base continua le persone impiegate per il trattamento in merito al rispetto dei requisiti della protezione dei dati.

4.7 In relazione al trattamento commissionato, il Fornitore deve assistere il Committente nella creazione e nell'aggiornamento del registro delle attività di trattamento e nell'esecuzione della valutazione d'impatto sulla protezione dei dati.

4.8 Se il Committente è soggetto a un controllo da parte delle autorità di controllo o da altri organismi oppure se gli interessati esercitano diritti nei confronti del Committente, il Fornitore si impegna a informare immediatamente il Committente e a fornire supporto nella misura necessaria relativamente al trattamento oggetto dell'incarico.

4.9 Il Fornitore può fornire informazioni a terzi o all'interessato solo con il previo consenso del Committente. Inoltre, il Fornitore informerà immediatamente il Committente eventuali richieste indirizzate direttamente al Fornitore.

4.10 Nella misura richiesta dalla legge, il Fornitore deve designare una persona competente e affidabile come responsabile della protezione dei dati. Occorre assicurarsi che le funzioni di tale responsabile non diano adito a conflitti di interesse. In caso di dubbio il Committente può contattare direttamente il responsabile della protezione dei dati. Il Fornitore comunica senza indugio al Committente i dati di contatto del responsabile della protezione dei dati o fornisce i motivi per cui non è stato nominato un responsabile. Il Fornitore comunica senza indugio al Committente qualsiasi cambiamento in merito alla persona o ai compiti interni del responsabile della protezione dei dati.

4.11 Il linea di principio il trattamento ha luogo all'interno dell'UE o dello SEE.

5. Misure tecniche e organizzative

5.1 Le misure di sicurezza dei dati descritte nell'Allegato 3 sono obbligatorie.

5.2 Le misure di sicurezza dei dati possono essere adattate in base agli sviluppi tecnici e organizzativi, a condizione che non siano inferiori al livello qui concordato. Il Fornitore deve implementare senza indugio qualsiasi modifica necessaria per mantenere la sicurezza delle informazioni. Il Committente sarà informato senza indugio di qualsiasi modifica. Eventuali modifiche sostanziali devono essere concordate tra le Parti.

5.3 Se le misure di sicurezza adottate non soddisfano o non soddisfano più le esigenze del Committente, il Fornitore ne informa immediatamente il Committente.

5.4 Il Fornitore assicura che i dati trattati nell'ambito dell'incarico siano rigorosamente separati da altri archivi di dati.

5.5 Eventuali copie o duplicati non possono essere redatti senza che il Committente ne sia a conoscenza. Fanno eccezione i duplicati temporanei tecnicamente necessari, nella misura in cui è esclusa una riduzione del livello di protezione dei dati qui concordato.

5.6 Il trattamento dei dati in abitazioni private è consentito. Laddove abbia luogo tale trattamento, il Fornitore provvede ad assicurare un livello di protezione e di sicurezza dei dati corrispondente al presente Contratto.

5.7 I supporti di dati dedicati, provenienti da o utilizzati per il Committente, sono contrassegnati in modo speciale e sono soggetti a una gestione continua. Devono essere conservati sempre in un luogo appropriato e non devono essere accessibili a persone non autorizzate. Vengono documentati gli accessi in entrata e in uscita.

6. Disposizioni su rettifica, cancellazione e blocco dei dati

6.1 Il Fornitore rettifica, cancella o blocca i dati trattati nell'ambito del suo incarico solo in conformità all'accordo contrattuale raggiunto o secondo le istruzioni del Committente.

6.2 Il Fornitore è tenuto a rispettare in ogni momento le istruzioni in merito del Committente. Eventuali servizi che non fanno parte dell'incarico originale saranno fatturati (per es. la conservazione dei dati).

7. Rapporti di subappalto

7.1 Il subappalto è consentito a condizione che i Subfornitori siano vincolati contrattualmente a obblighi di protezione dei dati almeno paragonabili a quelli concordati nel presente Contratto.

7.2 Le responsabilità del Fornitore e del Subfornitore devono essere chiaramente delimitate.

7.3 Sono consentiti ulteriori subappalti da parte del Subfornitore.

7.4 Il Fornitore seleziona accuratamente il Subfornitore con particolare riguardo all'idoneità delle misure tecniche e organizzative adottate dal Subfornitore.

7.5 Il ricorso a Subfornitori che non effettuano il trattamento di dati oggetto dell'incarico esclusivamente nel territorio dell'UE o del SEE è possibile solo se vengono rispettate le condizioni di cui all'articolo 5. È consentito, in particolare, nella misura in cui e fintantoché il Subfornitore offre adeguate garanzie di protezione dei dati.

7.6 Se il Subfornitore non rispetta i suoi obblighi in materia di protezione dei dati, il Fornitore ne risponde nei confronti del Committente.

7.7 Attualmente i Subfornitori designati nell'Allegato 1 con nome, indirizzo e natura dell'incarico si occupano del trattamento dei dati personali nella misura ivi specificata.

8. Diritti e obblighi del Committente

8.1 Il Committente è l'unico responsabile della valutazione della liceità del trattamento oggetto dell'incarico e della tutela dei diritti degli interessati.

8.2 Il Committente impartisce tutti gli incarichi, parti di incarichi o istruzioni in forma documentata. In casi urgenti le istruzioni possono essere impartite verbalmente. Tali istruzioni devono essere confermate senza indugio dal Committente in forma documentata.

8.3 Il Committente informa senza indugio il Fornitore qualora scopra errori o irregolarità nell'esame dei risultati dell'incarico.

8.4 Il Committente ha il diritto di controllare il rispetto delle norme sulla protezione dei dati e degli accordi contrattuali presso il Fornitore in misura ragionevole, direttamente o tramite terzi, in particolare acquisendo informazioni e controllando i dati conservati e i programmi di trattamento dei dati.

8.5 I controlli presso il Fornitore devono essere eseguiti senza interferenze evitabili sulla sua attività. A meno che non sia indicato diversamente per motivi urgenti da

documentare da parte del Committente, i controlli avranno luogo dopo un ragionevole preavviso e durante l'orario di lavoro del Fornitore, e con una frequenza non inferiore a 12 mesi. Il Fornitore può pretendere una remunerazione per consentire i controlli da parte del Committente.

9. Obblighi di notifica

9.1 Il Fornitore è tenuto a comunicare senza indugio al Committente qualsiasi violazione di dati personali. La comunicazione deve essere fatta al più tardi entro 24 ore dal momento in cui il Fornitore è venuto a conoscenza dell'evento in questione a un indirizzo designato dal Committente. Deve contenere almeno le seguenti informazioni:

- una descrizione della natura della violazione 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;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del Fornitore per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

9.2 Devono essere comunicate senza indugio anche le interruzioni sostanziali dell'esecuzione dell'incarico e le violazioni delle disposizioni sulla protezione dei dati o delle disposizioni del presente Contratto da parte del Fornitore o delle persone da lui impiegate.

9.3 Il Fornitore informa senza indugio il Committente su controlli o misure da parte delle autorità di controllo o di altri terzi, nella misura in cui questi riguardano il trattamento oggetto dell'incarico.

9.4 Il Fornitore assicura di fornire supporto al Committente nei suoi obblighi nella misura necessaria ai sensi dell'art. 32 e seguenti del regolamento generale sulla protezione dei dati.

10. Istruzioni

10.1 Il Committente si riserva un ampio diritto di impartire istruzioni in merito al trattamento oggetto dell'incarico.

10.2 Il Committente e il Fornitore designano nell'Allegato 2 le persone esclusivamente autorizzate a impartire e accettare istruzioni.

10.3 In caso di cambio o di impedimento a lungo termine delle persone designate, l'altra Parte deve essere informata senza indugio sul successore o sostituto.

10.4 Il Fornitore deve richiamare l'attenzione del Committente se, a suo parere, un'istruzione impartita dalla Committente viola le disposizioni di legge. Il Fornitore ha il diritto di sospendere l'esecuzione dell'istruzione in questione fino a quando non viene confermata o modificata dal titolare del trattamento presso il Committente.

11. Cessazione dell'incarico

11.1 Alla cessazione del rapporto contrattuale o in qualsiasi momento su richiesta del Committente, il Fornitore deve, a discrezione del Committente, distruggere o consegnare al Committente i dati trattati nell'ambito dell'incarico. Verranno distrutte altresì tutte le copie esistenti dei dati. La distruzione deve essere effettuata in modo tale che il ripristino anche di informazioni residue non sia più possibile con uno sforzo ragionevole.

11.2 Il Fornitore è obbligato ad effettuare la restituzione o cancellazione senza indugio anche nel caso di Subfornitori.

11.3 La documentazione che dimostra il corretto trattamento dei dati deve essere conservata dal Fornitore per i rispettivi periodi di conservazione anche dopo la fine del Contratto. Per sgravarsi da tale responsabilità, può consegnarla al Committente alla fine del Contratto.

12. Compenso

12.1 Il compenso del Fornitore è disciplinato in maniera definitiva nel Contratto principale.

13. Altro

13.1 Le Parti sono obbligate a trattare in modo confidenziale, anche dopo la cessazione del contratto, tutte le informazioni su segreti commerciali acquisite nell'ambito del rapporto contrattuale ed eventuali misure di sicurezza dei dati della controparte. Qualora ci fossero dubbi se un'informazione è soggetta all'obbligo di segretezza, essa sarà trattata in modo confidenziale fino a quando la controparte ne ammetterà l'uso non confidenziale per iscritto.

13.2 Qualora singole parti delle presenti Condizioni generali sul trattamento dei dati non fossero valide, ciò non pregiudica la validità delle altre parti.

13.3 Le presenti Condizioni generali sul trattamento dei dati costituiscono condizioni generali di contratto di No-Q srl ai sensi dell'articolo 1341 comma 1 del codice civile e sono efficaci nei confronti del Committente se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza.

13.4 Le presenti Condizioni generali sul trattamento dei dati sono disciplinate e interpretate ai sensi della legge applicabile nel territorio della Repubblica Italiana e qualsiasi controversia derivante dal Contratto sarà soggetta esclusivamente alla giurisdizione del tribunale di Bolzano.

Bressanone, il _____

Matthias Polig

Per il Fornitore

Luogo, data: _____

No-Q srl

Per il Committente

Allegato 1 – Subfornitori attualmente in essere

Servizi di hosting, di rete e di dati:

T-Systems-Sovereign Cloud powered by Google [GDPR](#)

Luogo del trattamento dei dati: UE

T-Systems International GmbH, Hahnstrasse 43d, D-60528 Frankfurt am Main. E-Mail: info@t-systems.com, telefono: +49 69 200 60-0

Amazon Web Services ([GDPR](#))

Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, Luxembourg City, 01855, Luxembourg

Luogo del trattamento dei dati: UE

Gestione delle chiavi crittografiche:

Thales ([GDPR](#))

Thales corporate headquarters, Tour Carpe Diem, 31 Place des Corolles, CS 20001 - 92098 Paris La Défense

Luogo del trattamento dei dati: UE

Web Application Firewall:

Cloudflare ([GDPR](#))

Cloudflare, Inc, 101 Townsend St, San Francisco, CA 94107, USA

Luogo del trattamento dei dati: Europa, USA

Garanzia di trattamento conforme al RGPD: Certificazione ISO/IEC 27701:2019

Monitoraggio delle prestazioni:

AppSignal ([GDPR](#))

AppSignal B.V., Rietwaard 4, 5236WC's Hertogenbosch, Paesi Bassi

Luogo del trattamento dei dati: UE

Servizio di posta elettronica:

Mailgun ([GDPR](#))

Mailgun Technologies, Inc, 112 E. Pecan St. #1135, San Antonio, TX 78205, USA

Luogo del trattamento dei dati: UE

SMTPeter ([GDPR](#))

Copernica BV, De Ruijterkade 112, 1011 AB, Amsterdam, Paesi Bassi

Luogo del trattamento dei dati: UE

Trasmissione opzionale dei risultati a Corona-Warn-App:

Corona-Warn-App

T-Systems International GmbH, Hahnstraße 43d, 60528, Frankfurt am Main, Germania

Luogo del trattamento dei dati: UE

Stampa e invio di Immune-ID:

pml GmbH, Arthur-Piechler-Str. 1i, 86316 Friedberg, Germania
<http://www.pml-augsburg.de/impressum/>

VENDO Kommunikation + Druck GmbH, Johannes Gutenbergstraße 2, 4840 Vöcklabruck,
Austria, <https://vendo.at/impressum>

Allegato 2 – Persone autorizzate a impartire istruzioni

Le seguenti persone sono autorizzate a impartire e accettare istruzioni:

Impartire:

si prega di compilare

Accettare:

Matthias Polig
Iiro Virtanen
Maria Hilber

Allegato 3 – Misure tecniche e organizzative

1 Riservatezza

- Controllo degli ingressi – misure per evitare che persone non autorizzate abbiano accesso ai supporti di dati che trattano o utilizzano dati personali: chiavi; finestre e porte di sicurezza a prova di scasso; scortare le persone nell'edificio aziendale;
- Controllo degli accessi – misure per prevenire l'uso non autorizzato del sistema: password; autenticazione a due fattori per gli accessi ai servizi del sistema;
- Controllo degli interventi – nessuna lettura, copia, modifica o rimozione non autorizzata all'interno del sistema grazie a: profili di autorizzazione che permettono un controllo differenziato degli accessi sui dati; registrazione degli accessi; archiviazione sicura dei supporti di memorizzazione; politica clear desk/clear screen.

2 Integrità dei dati

- Controllo dei trasferimenti – nessuna lettura, copia, modifica o rimozione non autorizzata durante la trasmissione elettronica o il trasporto grazie a: crittografia dei file; memorizzazione fisica sicura dei dati attraverso il cloud hosting;
- memorizzazione sicura: memorizzazione fisica sicura dei dati attraverso il cloud hosting; crittografia dei database e dei loro backup;
- Controllo degli inserimenti – determinare se e da chi i dati personali sono stati inseriti, modificati o rimossi dai sistemi di trattamento dei dati: registrazione; registri di dati, realizzabili a diversi livelli (per esempio sistema operativo, rete, firewall, database, applicazione); gestione dei documenti.

3 Disponibilità e resilienza

- Controllo della disponibilità – protezione contro la distruzione o la perdita accidentale o dolosa grazie a: strategia di backup (online/offline; on-site/off-site); antivirus; firewall;
- Possibilità di ripristino: i dati vengono salvati automaticamente ogni giorno e possono essere ripristinati in qualsiasi momento.

4 Procedura per testare, verificare e valutare regolarmente

- Gestione della protezione dei dati – valutazioni annuali e regolari della protezione dei dati per tutti i nostri servizi.
- Gestione della risposta agli incidenti: supporto nella risposta alle violazioni della sicurezza.
- Protezione dei dati per impostazioni predefinita: privacy by design/privacy by default;
- Controllo del trattamento: misure per garantire che i dati personali trattati per conto del cliente siano trattabili solo in conformità con le istruzioni del cliente. Tutti i fornitori e/o consulenti indipendenti si attengono alle linee guida definite per il trattamento dei dati.