Sada S.n.c. di Salini Daniele & C.

Strada alla Verza 21/M – 29122 Piacenza
Tel: 0523.713250 – info@sada.eu – info@pec.sada.eu
Website: www.sada.eu

CERTIFICATO DI CONFORMITA' GDPR

(General Data Protection Regulation – Reg.UE 2016 /679)

RELATIVO ALLA SOCIETA' NAQUADRIA SRL E SERVIZI DATACENTER

Il sottoscritto Dott. Luca Salini, in qualità di Data Protection Officer nominato dalla Società Naquadria Srl (Galleria Mirabello, 22 - 20081 Abbiategrasso MI - PIva: 08518080968) fornisce una sintetica evidenza degli elementi di conformità sviluppati dalla società, in relazione ai requisiti richiesti dalla normativa in oggetto.

Principi generali e liceità del trattamento (Art. 5 e 6 GDPR)

Tutti i dati personali trattati nell'ambito dei servizi erogati sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (limitazione della finalità);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
- esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione);
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

Ogni trattamento è legittimato da uno dei seguenti presupposti giuridici:

- l'interessato ha espresso il consenso al trattamento;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale o contrattuale;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

Trasparenza e diritti degli interessati (Art.12-23)

Naquadria adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

Ruoli e responsabilità (Art. 28, 29)

Naquadria ha fornito apposite istruzioni in merito al trattamento dei dati a tutti coloro che agiscono sotto la sua autorità. Qualora un trattamento dovesse essere esternalizzato si farà ricorso unicamente a responsabili esterni che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

Privacy by Default e Privacy by Design (Art.25)

Naquadria non è competente, né responsabile della quantità della e tipologia di dati inseriti da parte dei Clienti nelle proprie aree di archiviazione. Naquadria definisce lo sviluppo applicativo, l'applicazione di configurazioni ed impostazioni della propria infrastruttura mirate al rispetto dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, assicurando a tutte le aree di archiviazione le misure di sicurezza precedentemente descritte.

Sicurezza dei trattamenti (Art.32)

Naquadria adotta misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, ai dati personali conservati presso l'infrastruttura. Il sistema di sicurezza implementato comprende:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- ha implementato tecnologie, sistemi e policy volte alla sicurezza della rete (ex. Firewall, WAF,etc..), sicurezza dei sistemi (ex. monitoraggio dell'uso delle risorse, Sistema di monitoraggio del traffico tramite tool Cyber Command utilizzato internamente) e sicurezza gestionale (ex. applicazione di patch correttive e di sicurezza, backup) per la protezione dell'infrastruttura da utilizzi impropri o prevedibili rischi di sicurezza, essendo riconducibili a Naquadria le responsabilità relative al funzionamento del datacenter e delle piattaforme da essa esposti e definiti.

Si è ritenuto inoltre di certificare il proprio sistema di sicurezza delle informazioni secondo lo standard ISO/IEC 27001:2022 aumentato dalle linee guida per il Cloud ISO/IEC 27017:2015 e ISO/IEC 27018:2019 per i propri servizi cloud sia di tipo IaaS sia di tipo PaaS/SaaS.
Nel Corso degli anni sui Servizi cloud ha anche aggiunto la certificazione ISO 9001:2015 in modo da aver potuto chiedere, e poi ottenere, la qualifica come datacenter ed erogatore di servizi IaaS/PaaS/SaaS di ACN per il livello AI1 e QC1.

Data Breach (Art.33)

Si è sviluppata, anche nell'ambito dei sistema ISO 27001, una procedura per la gestione di eventuali incidenti di sicurezza, idonea a garantire i requisiti previsti dagli artt. 33 e 34 del GDPR (Data Breach). La procedura prevede, in caso di rilevazione di incidenti di sicurezza, la loro registrazione, la valutazione di rischio e l'eventuale comunicazione all'Autorità Garante ed agli interessati. Nel corso del 2025 tale procedura è stata integrata anche per il servizio NIS2/Csirt e vede oggi un percorso di gestione multipla degli incidenti con un tempo di notifica più stretto verso il CSIRT di 24 ore.

Privacy Impact Assessment (Art.35)

Qualora un tipo di trattamento dovesse presentare un rischio elevato per i diritti e le libertà delle persone fisiche, Naquadria effettuerà, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Tale valutazione prenderà in considerazione:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Trasferimento internazionale di dati (Art.44-47)

Le infrastrutture adibite all'erogazione dei servizi di Naquadria e partner sono collocate in Italia, escludendo di norma un trasferimento di dati verso paesi non appartenenti alla UE. Qualora dovesse rendersi necessario valutare trasferimenti internazionali di dati, verranno rispettate le rispettive disposizioni:

- trasferimento sulla base di una decisione di adeguatezza;
- trasferimento soggetto ad adeguate garanzie;
- norme vincolanti di impresa.

Piacenza, 13.07.2026

Dott. Luca Salini – Sada S.n.c.
Luca Salini
13.07.2026 16:56:57
GMT+02:00