Protocollo di sicurezza e protezione dati

(Riferimento ai principi del D.Lgs. 138/2024 attuativo Direttiva (UE) 2022/2555 – NIS2)

Sommario

1. Premessa – Standard di sicurezza

Veronafiere S.p.A. (di seguito "**Veronafiere**"), pur non rientrando formalmente tra i soggetti obbligati ai sensi del D.Lgs. 138/2024 (attuativo della Direttiva (UE) 2022/2555 – "NIS2"), adotta volontariamente principi, misure e modelli organizzativi coerenti con tali disposizioni, quale standard interno di riferimento per la gestione dei rischi informatici e la protezione dei dati.

L'accesso a sistemi o informazioni di proprietà di Veronafiere viene concesso al Soggetto Terzo identificato come Segreteria Organizzativa Esterna o Fornitore (di seguito "**Società**") è pertanto subordinato al rispetto di tali principi.

2. Responsabilità al trattamento

La Società è tenuta, qualora nel rapporto con Veronafiere sia previsto il trattamento di dati personali o grandi quantità di dati (di qualsiasi natura) di proprietà di Veronafiere, alla compilazione di un questionario condiviso da Veronafiere per una preliminare analisi del rischio. A seguito della compilazione, Veronafiere può sottoporre alla Società una nomina a responsabile esterno al

trattamento (ex Art. 28 GDPR – Responsabile del trattamento) o DPA (Data Processing Agreement) per delineare:

- istruzioni;
- misure di sicurezza;
- limiti d'uso;
- durata;
- analisi dei rischi;
- gestione dei sub-responsabili.

3. Oggetto dell'accesso

L'accesso è concesso esclusivamente per finalità connesse all'esecuzione dell'incarico affidato e limitatamente alle funzionalità e ai dati espressamente abilitati da Veronafiere secondo criteri di:

- minimizzazione dei privilegi (least privilege);
- separazione dei ruoli;
- necessità operativa.

L'accesso costituisce concessione revocabile e non attribuisce alcun diritto autonomo sui dati visualizzati.

4. Gestione degli account e tracciabilità

L'accesso avviene esclusivamente mediante:

- account nominali individuali e non cedibili
- Eventuali account condivisi devono essere preventivamente autorizzati da Veronafiere. In tali casi, la Società è responsabile di garantire la tracciabilità degli accessi, mantenendo registrazione aggiornata dei soggetti che utilizzano tali credenziali e delle relative attività svolte;
- autenticazione multifattore, ove prevista.

È consigliato l'utilizzo di una VPN.

È vietato l'utilizzo di account condivisi.

La Società è responsabile:

- della custodia delle credenziali;
- della corretta gestione degli accessi interni;
- dell'immediata comunicazione di cessazioni o variazioni del personale autorizzato;

Tutte le attività sono soggette a tracciamento (logging) e conservazione dei log secondo le politiche interne di sicurezza di Veronafiere.

5. Obblighi di sicurezza informatica (principi NIS2)

In coerenza con i principi di gestione del rischio e sicurezza delle reti e dei sistemi informativi previsti dalla Direttiva di riferimento NIS2, la Società garantisce di adottare misure tecniche e organizzative adeguate, tra cui almeno:

- utilizzo di dispositivi aziendali protetti da autenticazione individuale;
- aggiornamento periodico di sistemi operativi e software;
- protezione endpoint (antivirus/antimalware attivo);
- firewall e protezioni di rete adeguate;
- divieto di accesso tramite reti pubbliche non protette (possibilmente tramite VPN);
- policy interne di gestione password robuste;
    - minimo 12 caratteri (lettere maiuscole e minuscole, numeri, carattere speciali);
- formazione minima del personale sui rischi di phishing, social engineering e compromissione credenziali;
- segregazione dei dati eventualmente esportati e cifratura degli stessi;
- sistema di conservazione dei log.

la Società si impegna a garantire che i propri sistemi non costituiscano fattore di vulnerabilità per l'infrastruttura di Veronafiere.

6. Incidenti di sicurezza e obbligo di notifica

In caso di:

- sospetta compromissione credenziali;
- accesso non autorizzato;
- perdita o diffusione di dati;
- evento che possa incidere sulla sicurezza dei sistemi o delle informazioni di Veronafiere;

la Società è tenuta a darne comunicazione a Veronafiere senza ingiustificato ritardo e comunque entro 24 ore dalla scoperta dell'evento. Inoltre, la Società è tenuta a fornire a Veronafiere ogni evidenza, log o statistica relativa all'incidente entro 48 ore dalla scoperta dell'evento.

Veronafiere si riserva di adottare misure immediate di sospensione o revoca degli accessi.

7. Protezione dei dati personali – GDPR

Qualora l'accesso comporti trattamento di dati personali, la Società:

- opera nel rispetto del Regolamento (UE) 2016/679 (GDPR);
- tratta i dati esclusivamente per le finalità contrattuali;
- non effettua comunicazioni o trattamenti ulteriori non autorizzati;
- adotta misure tecniche e organizzative adeguate al rischio;
- conserva i dati, qualora previsto, per la sola durata contrattuale del rapporto con Veronafiere. A fine incarico è prevista una restituzione o cancellazione del dato trattato.

Le Parti disciplineranno, ove necessario, il ruolo privacy (Responsabile del trattamento ex art. 28 GDPR o diverso inquadramento).

8. Limitazioni su esportazione e utilizzo dati

L'accesso alle informazioni di Veronafiere è concesso esclusivamente per le finalità connesse alle attività affidate. È pertanto vietato accedere, consultare o generare estrazioni di dati non strettamente necessari o non rientranti nella propria competenza operativa, incluse a titolo esemplificativo le anagrafiche e altri dati gestionali non pertinenti alle attività assegnate.

In particolare, è vietato:

- esportare dati senza preventiva autorizzazione scritta di Veronafiere;
- creare copie locali non autorizzate;
- utilizzare i dati per finalità diverse da quelle contrattuali;
- condividere credenziali o informazioni con soggetti terzi;

Eventuali esportazioni autorizzate dovranno avvenire con adeguate misure di protezione (cifratura, accesso controllato, conservazione limitata).

9. Utilizzo di caselle di posta elettronica di Veronafiere

Qualora Veronafiere decida di mettere a disposizione della Società una o più caselle di posta elettronica con domini di proprietà di Veronafiere, le stesse dovranno essere utilizzate esclusivamente per finalità connesse all'esecuzione del contratto.

La Società si impegna a:

- non utilizzare la casella per finalità personali o estranee all'incarico;
- non attivare servizi esterni collegati alla casella senza preventiva autorizzazione scritta di Veronafiere;
- rispettare le policy aziendali in materia di sicurezza informatica, protezione dei dati e conservazione delle informazioni;
- adottare adeguate misure di sicurezza per la protezione delle credenziali (divieto di condivisione password, obbligo di autenticazione forte ove prevista).

Veronafiere si riserva il diritto di:

- monitorare, nei limiti consentiti dalla normativa vigente, l'utilizzo delle caselle per finalità di sicurezza e tutela del patrimonio informativo;
- sospendere o revocare in qualsiasi momento l'accesso in caso di utilizzo non conforme o cessazione del rapporto contrattuale.

Alla cessazione del contratto, l'accesso sarà disabilitato e Veronafiere potrà trattenere i contenuti per esigenze organizzative, legali o di continuità operativa, nel rispetto della normativa applicabile.

10. Utilizzo di dispositivi di Veronafiere

Qualora Veronafiere decida di assegnare alla Società un notebook o altri dispositivi informatici aziendali, tali strumenti restano di esclusiva proprietà di Veronafiere e sono concessi in uso esclusivamente per l'esecuzione delle attività oggetto del contratto.

La Società si impegna a:

- utilizzare i dispositivi esclusivamente per finalità professionali connesse all'incarico;
- non modificare configurazioni di sicurezza, sistemi di protezione o strumenti di monitoraggio;
- garantire la custodia diligente del dispositivo e prevenire accessi non autorizzati;
- segnalare tempestivamente eventuali incidenti di sicurezza, smarrimento o furto.

È fatto divieto di:

- utilizzare dispositivi personali in sostituzione senza autorizzazione (salvo diverso accordo scritto);
- copiare o trasferire dati aziendali su supporti esterni non autorizzati;
- disabilitare sistemi di cifratura, antivirus o soluzioni di endpoint protection installate;
- compromettere la sicurezza del dispositivo attraverso download di software di dubbia natura o installazione di programmi senza la supervisione di Veronafiere.

Veronafiere si riserva la facoltà di:

- applicare policy di monitoraggio, logging e controllo tecnico sui dispositivi assegnati, nei limiti consentiti dalla normativa vigente;
- effettuare aggiornamenti, patch di sicurezza o interventi tecnici da remoto e/o una richiesta di intervento in presenza sul notebook di proprietà;
- richiedere in qualsiasi momento la restituzione del dispositivo.

Alla cessazione del rapporto contrattuale, la Società è tenuta a restituire immediatamente i dispositivi assegnati, integri e completi di accessori, fatto salvo il normale deterioramento d'uso.

11. Condivisione dati

La Società si impegna, per tutta la durata del rapporto contrattuale, a utilizzare esclusivamente i sistemi e le piattaforme di condivisione documentale indicati da Veronafiere, attualmente identificati in Microsoft OneDrive.

È fatto espresso divieto di utilizzare strumenti alternativi di condivisione (a titolo esemplificativo e non esaustivo: servizi cloud personali, piattaforme di file sharing non autorizzate, supporti esterni non approvati) per la gestione di documenti, dati, informazioni o materiali riconducibili alle attività svolte per conto di Veronafiere.

12. Controlli e audit

Veronafiere si riserva la facoltà di:

- effettuare verifiche sull'utilizzo degli accessi;
- richiedere evidenza delle misure di sicurezza adottate;
- sospendere o revocare gli accessi in caso di utilizzo non conforme.

13. Responsabilità e manleva

La Società è responsabile per ogni utilizzo improprio degli accessi e per eventuali danni, sanzioni o violazioni normative derivanti da condotte proprie o dei propri incaricati.

La Società si impegna a manlevare e tenere indenne Veronafiere da ogni conseguenza pregiudizievole derivante da violazioni degli obblighi di cui alla presente clausola.