ATTESTATO DI CONFORMITA' PRIVACY E PROTEZIONE DEI DATI

REDATTO DA: **Galli Data Service Srl** (Data Protection Officer)	APPROVATO DA: **Gruppo Vetreria di Borgonovo*** (Data Controller)
GALLI DATA SERVICE SRL Strada della Viggioletta, 8 29121 Piacenza C.F. e P.I. 01690860331	Vetreria di Borgonovo S.p.A. Uff. e Amm.: Via Pianello, 75 29011 BORGONOVO V.T. (PC) Tel. 0523.865311 - Fax 0523.862843
..... (Timbro/Firma)	..... (Timbro/Firma)

** Con il termine "Gruppo Vetreria di Borgonovo" o "Gruppo" si intendono le società: Vetreria di Borgonovo Spa, Decover Srl, Valentina 96 Spa. Le società Vetreria di Borgonovo e Decover operano nel settore della produzione, decorazione e vendita di prodotti in vetro; Valentina 96, la società capofila, fornisce servizi in area amministrativa, organizzativa, informatica. Il Gruppo, utilizzando sistemi informativi comuni, condivide le medesime politiche in termini di sicurezza dei dati e conformità privacy. Il presente attestato è redatto da una società di consulenza esterna, Galli Data Service Srl, che rivesta la carica di Responsabile della protezione dei dati per la società capofila del Gruppo.*

INDICE

1) Scopo del documento

Il presente documento è finalizzato a presentare i principali elementi di conformità privacy e protezione dei dati adottati dal Gruppo. Il presente attestato rappresenta una sintesi, ottimizzata per la diffusione agli stakeholders, del Modello di Accountability, un documento, ad uso interno, che definisce i dettagli di recepimento delle vigenti normative a tutela dei dati. Il presente attestato è rilasciato da Galli Data Service Srl (società che si occupa di servizi di compliance), rappresentando una certificazione di terza parte, in merito alle politiche di data protection del Gruppo. La Direzione del Gruppo è coinvolta nel rispetto e nell'attuazione dei contenuti del presente attestato, assicurando e verificando periodicamente che l'impegno alla tutela dei dati sia documentato, reso operante, riesaminato, migliorato e diffuso a tutto il personale.

2) Principi generali ed obiettivi

La "Conformità privacy e protezione dei dati" sono parti integranti del patrimonio del Gruppo, rappresentando un valore primario dell'attività e della crescita aziendale.

2.1) Sicurezza dei dati

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite dal Gruppo. La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, nonché danni di natura economica e finanziaria. Le informazioni rappresentano dunque un patrimonio di grande valore ed un bene da tutelare, adottando procedure e comportamenti atti a garantirne la salvaguardia. Il Gruppo intende pertanto assicurare:

- la confidenzialità delle informazioni (le informazioni devono essere accessibili solo da chi è autorizzato);
- l'integrità delle informazioni (protezione dell'esattezza, della precisione e della completezza delle informazioni e dei metodi per la loro elaborazione);
- la disponibilità delle informazioni (gli utenti autorizzati devono poter effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono).

2.2) Conformità privacy (la protezione dei dati personali)

Per dati personali si intendono tutte le informazioni riconducibili, direttamente o indirettamente, ad una persona fisica. La corretta gestione e tutela dei dati personali consente al Gruppo di: erogare servizi rispettando un adeguato standard qualitativo; scongiurare il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti; incentivare la relazione con gli stakeholedrs, attraverso garanzie di affidabilità. Il Gruppo si impegna a:

- rispettare l'identità, la personalità, la dignità di ogni soggetto con cui si interfaccia, nonché la sfera personale e la vita privata di ognuno;
- proteggere i dati personali di ogni individuo;
- rispettare le libertà fondamentali in tema di privacy, anche attraverso la garanzia della conformità legislativa (Reg.UE 2016/679 e D.Lgs.196/2003, come modificato ed integrato da D.Lgs.101/2018);
- ridurre l'utilizzo di dati personali al minimo necessario essenziale per il raggiungimento delle finalità dichiarate;

- limitare il trattamento dei dati personali solo a quelli pertinenti a finalità determinate, esplicite e legittime, con modalità, strumenti e limiti di conservazione proporzionati alle finalità da raggiungere;
- fornire all'interessato informazioni e comunicazioni aggiornate, facilmente accessibili e comprensibili relative al trattamento dei suoi dati personali;
- garantire la correttezza e attendibilità dei dati trattati, attraverso la loro verifica e aggiornamento;
- garantire i diritti degli interessati previsti in materia di privacy.

3) Ruoli e responsabilità

3.1) Titolare del trattamento

Ogni società del Gruppo, in persona dell'organo di rappresentanza pro-tempore, riveste la carica di Titolare del trattamento, esercitando il potere decisionale circa le finalità ed i mezzi del trattamento. Il Gruppo ha sviluppato un sistema di conformità privacy integrato, basato sulla condivisione di modelli documentali e sull'utilizzo di sistemi informativi comuni.

3.2) Responsabile della protezione dei dati

Indipendentemente dalla cogenza della nomina, in riferimento agli Art.37-39 del GDPR, la società capofila ha deciso di designare il Responsabile della Protezione dei Dati (RPD o DPO). Il DPO è una società di consulenza esterna (Galli Data Service Srl), specializzata in servizi di conformità normativa. Il DPO è coinvolto, tempestivamente e adeguatamente, in tutte le questioni riguardanti la protezione dei dati personali. Il DPO, sulla base delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, garantisce al Titolare un adeguato supporto per una corretta applicazione del GDPR, nonché per la scelta di adeguate misure di sicurezza a tutela dei dati.

3.3) Coordinatori privacy

Il Gruppo ha deciso di nominare due "Coordinatori Privacy" all'interno dello staff operativo, al fine di garantire un adeguato e fattivo coordinamento tra il DPO e l'operatività quotidiana aziendale:

- HR Manager (al fine di gestire gli adempimenti connessi alle risorse umane);
- IT Manager (al fine di gestire gli adempimenti connessi ai sistemi informatici).

3.4) Persone autorizzate al trattamento

Il Gruppo procede a nominare quale "Autorizzato al trattamento" qualsiasi persona che tratta dati personali, di norma gli impiegati / operatori dotati di profilo informatico individuale. L'atto di nomina contiene:

- ambito del trattamento consentito (attività, categorie di dati, finalità del trattamento);
- istruzioni per un corretto trattamento (di norma integrate con eventuali piani di formazione specifici).

3.5) Responsabili e sub-responsabili esterni del trattamento

Il Gruppo nomina quali responsabili esterni tutti i soggetti a cui viene esternalizzata un'attività di trattamento (es: fornitori/consulenti in ambito HR, in ambito amministrativo, in ambito IT, ecc.) Sono nominati solo soggetti che prestino adeguate garanzie di affidabilità, in termini di protezione e riservatezza dei dati. I Responsabili esterni possono avvalersi di sub-responsabili solamente se prestano le medesime garanzie a loro richieste. Nel caso in cui una società del Gruppo fosse nominata Responsabile esterno, avrà cura di rispettare le istruzioni fornite dal Titolare.

4) Mappatura dei dati e valutazione dei rischi

Al fine di applicare correttamente il principio di "Accountability", sancito dall'Art.5 del GDPR, il Gruppo sviluppa e documenta le seguenti attività:

- analisi di contesto (mappatura degli elementi significativi in merito alla tutela dei dati, per esempio: inventario dei sistemi informatici coinvolti, analisi organigramma funzionale, ecc.);
- tenuta del registro dei trattamenti (mappatura delle attività di trattamento effettuate);
- analisi dei rischi (identificazione del rischio, di varia probabilità e gravità, di impatto negativo per i diritti e le libertà delle persone fisiche);
- principi di privacy by default e by design (identificazione dei requisiti di conformità da valutare in via preventiva all'inizio di nuove attività di trattamento);
- tempo di conservazione dei dati (identificazione di un criterio che definisca il periodo di conservazione dei dati);
- trasferimenti extra UE (identificazione di eventuali trasferimenti fuori dalla Unione Europea e correlate basi giuridiche);
- principi di liceità del trattamento (identificazione delle basi legali su cui si fondano i singoli trattamenti).

La seguente tabella identifica la metodologia di classificazione dei suddetti elementi, adottata dalle società del Gruppo (le tabelle compilate sono inserite nel documento, ad uso interno, chiamato "Modello di Accountability").

ATTIVITA' DI TRATTAMENTO	**Nome**			
	Descrizione			
PROFILI DEL TRATTAMENTO	**Categorie di dati**			
	Soggetti interessati			
	Finalità del trattamento			
	Tempo conservazione			
SOGGETTI COINVOLTI	**Soggetti autorizzati**			
	Responsabili esterni			
	Contitolari			
	Diffusione			
	Trasferimenti all'estero			
	Base del trasferimento			
STRUMENTI	**Repository**			
	Asset			
CALCOLO DEL LIVELLO DI RISCHIO E VALUTAZIONI DI IMPATTO	**GRAVITA'**			
	PROBABILITA'			
	RISCHIO TOTALE			
	CRITERI PIA			
PRINCIPI DI LICEITA' E SICUREZZA	**Liceità del trattamento**			
	Privacy by design/default			
	Misure di sicurezza specifiche			
VALUTAZIONE FINALE		Il trattamento può iniziare / continuare (rischio mitigato da piano di sicurezza)	Trattamento da sottoporre ad ulteriori valutazioni di impatto	Trattamento da sottoporre a consultazione preventiva dell'Autorità Garante
NOTE				

5) Misure di sicurezza

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento (ai sensi dell'Art.32 del GDPR), il Gruppo implementa misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali 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.

I seguenti paragrafi forniscono evidenze di dettaglio circa le misure di sicurezza, adottate con riferimento agli standard internazionali di sicurezza, quali la ISO/IEC 27001:2013.

5.1) Procedure di autenticazione ed autorizzazione

Si adottano le seguenti misure di autenticazione ed autorizzazione:

- l'accesso ai profili utente avviene per mezzo di un sistema di autenticazione basato su user e password;
- le password sono vincolate a criteri di complessità e sostituzione periodica;
- ad ogni utente è associato un profilo individuale;
- i privilegi di accesso agli applicativi / alle share di rete / ai dati sono segregati in relazione alla mansione lavorativa;
- esiste una modalità predefinita per la disattivazione degli utenti, riconsegna dotazioni, gestione dati;
- i ruoli con privilegi speciali (admin) sono chiaramente definiti ed assegnati ad un numero ristretto di utenti, oggetto di istruzioni specifiche e monitoraggio attività.

5.2) Sicurezza perimetrale, delle reti e protezione da malware

Si adottano le seguenti misure di sicurezza:

- computer e servers sono protetti da specifica soluzione antivirus (ESET Antivirus);
- il traffico di rete è gestito / protetto da specifica soluzione firewall (Kerio);
- gli apparati di sicurezza sono dotati di specifiche protezioni da ransomware / soluzioni IDS/IPS/DLP;
- si adottano soluzioni di webfiltering (Kerio Web Filtering) con blocco automatico di categorie di siti web considerate a rischio;
- le reti sono segmentate e si utilizzano DMZ per servizi esposti ad internet;
- le reti wireless sono segmentate (interna, guests, etc.) e protette da password, periodcamente sostituita (6 mesi);
- specifici controlli e strumenti di sicurezza, per esempio multi-factor authentication, sono adottati per le connessioni remote (vpn).

5.3) Sicurezza di computer e server

Si adottano le seguenti misure di sicurezza:

- gli utenti non hanno privilegi di admin sulle macchine (che gli consentano di bypassare/modificare le configurazioni preimpostate o installare applicativi);
- i sistemi attivano time-out di sessione (screen-saver con password) se l'utente rimane inattivo un certo periodo di tempo (10 minuti);

- si adottano sistemi di cifratura per le unità di memoria dei notebook;
- l'accesso alla sala server è monitorato e consento solo tramite badge;
- si adottano sistemi di sicurezza dedicati per la sala server (antincendio, antiallagamento, controllo tensione elettrica, ecc.);
- si adottano sistemi di cancellazione sicura dati o distruzione fisica memoria da utilizzarsi in caso di smaltimento o reimpiego di strumenti contenenti dati personali.

5.4) Sicurezza applicativi, web-site, e-mail

Si adottano le seguenti misure di sicurezza:

- gli aggiornamenti dei sistemi operativi ed applicativi sono regolarmente installati (patching);
- gli applicativi critici sono dotati di specifici ulteriori sistemi di autenticazione ed autorizzazione;
- gli applicativi esposti ad internet e/o il sito web sono dotati di certificati SSL;
- i database degli applicativi critici e/o del sito web sono cifrati (encryption);
- si effettua una valutazione di affidabilità per i servizi cloud utilizzati (evidenza sul collocamento dei server; adeguate garanzie contrattuali di servizio, SLA, ecc.);
- la posta elettronica è soggetta a procedura di autenticazione ed è dotata di funzioni antipsam, sistemi di trasmissione sicura, sistemi di back-up, sistemi di disabilitazione in caso di cessazione utente, disclamier e risponditori automatici, ecc.;
- vengono effettuati, da terze parti, interventi di vulnerability assessment / penetration test;
- esiste un sistema di monitoraggio continuo (Safetica) della sicurezza dei sistemi IT, della performance e delle attività degli utenti;
- si utilizzano sistemi di log management per monitoraggio degli accessi amministrativi, navigazione web, uso vpn, uso di unità di memoria removibili, ecc.

5.5) Sicurezza di strumenti di condivisione (multifunzione, memorie, cloud repositories)

Si adottano le seguenti misure di sicurezza:

- esistono sistemi di protezione delle stampanti comuni (es: stampa con PIN);
- gli strumenti scanner possono inviare i file direttamente ad indirizzi email o aree segregate;
- si utilizzano strumenti tracciabili per la gestione di fax;
- le unità di memoria removibili (es: USB flashpen, unità ottiche, hard disk esterni, ecc.) sono automaticamente analizzate dai sistemi di sicurezza;
- si utilizzano sistemi di condivisione cloud sicuri (soluzioni interne monitorate).

5.6) Sicurezza dei mobile-device

Si adottano le seguenti misure di sicurezza:

- attivazione Sim-Card PIN;
- attivazione procedure di autenticazione;
- tempi di time-out di sessione prestabiliti;
- utilizzo di soluzione MDM che consente una gestione remotizzata ed accentrata dei device.

5.7) Sistemi di back-up e ripristino

Si adottano le seguenti misure di sicurezza:

- si utilizzano soluzioni automatiche per un back-up completo dei dati aziendali;
- i sistemi di back-up forniscono alert di evidenza di buon fine delle operazioni;
- si utilizzano unità di memoria dedicate al back-up (NAS);
- le copie di back-up sono collocate in luoghi ragionevolmente distanti dalla sala server;
- l'infrastruttura di virtualizzazione è replicata in apposito data-center;

- sono presenti procedure di back-up, disaster recovery, business continuity;
- si effettuano attività di ripristino su richiesta e programmate.

5.8) Misure di sicurezza organizzative

Si adottano le seguenti misure di sicurezza:

- esiste un inventario delle infrastrutture e sistemi IT;
- è definita una configurazione standard dei sistemi ed una procedura per richiedere/effettuare modifiche;
- esiste una procedura di gestione degli incidenti di sicurezza (si veda inoltre par.6);
- si utilizza una piattaforma software dedicata alla gestione del sistema di conformità;
- si divulgano adeguate informative a tutti i soggetti che conferiscono dati personali (si veda inoltre par.7.1);
- si adottano apposite procedure / modulistica per garantire l'esercizio dei diritti degli interessati (si veda inoltre par.7.2);
- tutti i soggetti (interni ed esterni che trattano dati personali sono appositamente nominati ed istruiti (si veda inoltra par.3).

5.9) Misure di sicurezza fisica

Si adottano le seguenti misure di sicurezza:

- la sede fisica è perimetrata e dotata di accessi sicuri;
- l'assegnazione delle chiavi di accesso è controllata;
- i visitatori sono registrati ed accolti in apposite aree o locali;
- la sede è dotata di impianto di allarme e videosorveglianza;
- accessi e porte degli uffici, nonché alcuni armadi, sono dotati di serratura;
- la documentazione contenente dati critici è conservata in supporti protetti e separati;
- i dispositivi hardware critici (es: strumenti di firma, token home-banking, ecc.) sono conservati in modalità sicura;
- il personale è istruito sulla corretta gestione dei documenti e degli spazi lavorativi;
- postazioni e monitor sono orientati in modo da prevenire la visibilità occasionale di soggetti non autorizzati;
- si evita l'esposizione di dati confidenziali su bacheche / copertine raccoglitori, ecc.;
- i locali adibiti ad archivio sono adeguatamente protetti;
- si utilizzano strumenti distruggi-documenti prima di smaltire supporti cartacei contenenti dati critici.

6) Gestione incidenti di sicurezza

In conformità alle prescrizioni di cui agli articoli 33,34 del GDPR, il Gruppo mantiene un registro di qualsiasi evento che possa compromettere la sicurezza dei dati (inteso come violazione che possa causare la distruzione, la perdita, la modifica, la divulgazione/accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati). Il registro data breach contiene:

- una descrizione della natura della violazione, comprendente, 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;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Se necessario, Il Gruppo comunica prontamente le suddette informazioni all'Autorità di controllo, agli interessati ed agli stakeholders coinvolti.

7) Misure di trasparenza

Il Gruppo adotta adeguate misure per fornire agli interessati le informazioni previste dagli articoli 13,14 del GDPR (informative privacy) e dagli articoli 15-21 (diritti degli interessati) in forma sintetica, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici.

7.1) Informative privacy

Il Gruppo rende disponibili agli interessati, nelle modalità previste dalla normativa, tutte le informazioni di cui agli articoli 13 e 14 del GDPR, tra cui: dettagli di contatto del Titolare e del DPO, finalità e basi giuridiche del trattamento, ambito di conoscibilità dei dati, ecc.

7.2) Diritti degli interessati

Il Gruppo ha sviluppato un'apposita procedura per agevolare gli interessati nell'esercizio dei diritti garantiti dagli articoli 15-21 del GDPR: diritto di accesso, rettifica, cancellazione, limitazione, portabilità, opposizione.

8) Controlli ed aggiornamenti

La seguente tabella identifica le modalità di aggiornamento del sistema di conformità privacy:

PROFILO DA AGGIORNARE	REF. GDPR	TEMPISTICA DI CONTROLLO / AGGIORNAMENTO
Data Breach Incidente di sicurezza	Art.33 GDPR	• Registrazione e valutazione immediata • Notifica entro 72 ore (se prevista)
Privacy by design Gestione di nuovi processi, tecnologie, trattamenti	Art.25 GDPR	• Prima dell'inizio del trattamento
Privacy Impact Assessment (PIA) Gestione di trattamenti critici	Art.35 GDPR	• Prima dell'inizio del trattamento
Diritto di accesso Risposta a richieste degli interessati	Art.15 GDPR	• Entro 1 mese dalla richiesta
Raccolta dati da terze parti Gestione dell'informativa	Art.14 GDPR	• Entro 1 mese dalla raccolta
Analisi di contesto Registrazione cambiamenti strutturali	Art.24 GDPR	• Qualora necessario (in caso di variazioni)
Registro dei trattamenti Insertion of new data processing	Art. 30 GDPR	• Qualora necessario (in caso di variazioni)
Analisi dei rischi Valutazione e revisione periodica	Art.32 GDPR	• Audit annuale
Verifica piano sicurezza Verifica efficacia delle misure	Art.32 GDPR	• Audit annuale
Autorizzazione ed istruzioni Nomina di nuovi dipendenti	Art.29 GDPR	• In occasione dell'inizio del rapporto lavorativo
Nomina responsabili esterni Nomina di nuovi consulenti/fornitori	Art.28 GDPR	• In occasione dell'inizio del rapporto professionale

Il presente attestato è reso disponibile agli stakeholders ed aggiornato mediante la sua pubblicazione sul sito web istituzionale di Gruppo.