Ferrari Spa

VERBALE DI AUDIT COMPLIANCE GDPR

Data Sessione: 06/01/2026 17:35

Rating Conformità: 32,5%

Creato da: Martina Lonardi

Data Export: 06/01/2026

1. Governance e Responsabilità (Accountability)

L'azienda ha identificato e formalizzato chi è il "Titolare del Trattamento" (solitamente l'azienda stessa)? (Sì/No)

Esito: **CONFORME (SÌ)**

È stato nominato un Responsabile della Protezione dei Dati (DPO/RPD), sia interno che esterno? (Sì/No)

Esito: **CONFORME (SÌ)**

Esiste una politica privacy interna (un regolamento) comunicata a tutti i dipendenti? (Sì/No)

Esito: **CONFORME (SÌ)**

Tutti i dipendenti e collaboratori che trattano dati hanno ricevuto una formazione base sul GDPR? (Sì/No)

Esito: **CONFORME (SÌ)**

Sono state distribuite e firmate le "lettere di autorizzazione" (o incarico) per il personale che tratta dati? (Sì/No)

Esito: **CONFORME (SÌ)**

L'azienda documenta le proprie scelte e valutazioni in materia di privacy (es. verbali, analisi)? (Sì/No)

Esito: **NON CONFORME (NO)**

2. Mappatura e Registro dei Trattamenti

È stato redatto e viene mantenuto aggiornato il "Registro delle Attività di Trattamento"? (Sì/No)

Esito: **NON CONFORME (NO)**

Il Registro elenca chiaramente perché i dati vengono raccolti (le finalità)? (Sì/No)

Esito: **NON CONFORME (NO)**

Il Registro elenca quali categorie di dati vengono raccolte (es. anagrafici, bancari, sanitari)? (Sì/No)

Esito: **NON CONFORME (NO)**

Il Registro indica per quanto tempo i dati vengono conservati (tempi di conservazione)? (Sì/No)

Esito: **NON CONFORME (NO)**

Sono stati mappati i flussi di dati (sappiamo dove vanno i dati, chi li vede)? (Sì/No)

Esito: **NON CONFORME (NO)**

3. Basi Giuridiche e Informative

Per ogni trattamento nel Registro, è stata identificata una base giuridica valida (es. contratto, consenso, obbligo legale)?

Esito: **NON CONFORME (NO)**

L'azienda ha un'informativa privacy (policy) aggiornata sul proprio sito web? (Sì/No)

Esito: **CONFORME (SÌ)**

L'azienda fornisce un'informativa specifica ai propri dipendenti? (Sì/No)

Esito: **CONFORME (SÌ)**

L'azienda fornisce un'informativa specifica ai propri clienti/utenti? (Sì/No)

Esito: **CONFORME (SÌ)**

Quando si chiede il consenso (es. per il marketing), questo è separato da altre richieste (es. accettazione contratto)? (Sì/No)

Esito: **CONFORME (SÌ)**

Esiste un sistema per registrare e dimostrare il consenso (es. data, ora, testo dell'informativa) ricevuto? (Sì/No)

Esito: **CONFORME (SÌ)**

4. Diritti degli Interessati

Esiste una procedura chiara e un referente interno per gestire le richieste degli interessati (es. richiesta di accesso, cancellazione)? (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda ha un indirizzo email o un modulo dedicato (e indicato nelle informative) per l'esercizio dei diritti? (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda è tecnicamente in grado di trovare tutti i dati di una persona che ne fa richiesta? (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda è tecnicamente in grado di cancellare (diritto all'oblio) i dati di una persona, dove previsto dalla legge? (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda è in grado di rispondere a una richiesta entro i termini di legge (30 giorni)? (Sì/No)

Esito: **NON CONFORME (NO)**

5. Sicurezza e Data Breach

Esistono misure di sicurezza di base (es. antivirus aggiornati, firewall) sui dispositivi aziendali? (Sì/No)

Esito: **CONFORME (SÌ)**

I dati sensibili o critici sono protetti da crittografia (es. sui dischi dei portatili, su cloud)? (Sì/No)

Esito: **NON CONFORME (NO)**

L'accesso ai dati è limitato solo al personale che ne ha effettivamente bisogno per lavorare? (Sì/No)

Esito: **CONFORME (SÌ)**

Esiste una policy per la gestione delle password (es. complessità, cambio regolare)? (Sì/No)

Esito: **CONFORME (SÌ)**

Vengono eseguiti backup regolari dei dati? (Sì/No)

Esito: **NON CONFORME (NO)**

Esiste una procedura scritta da seguire in caso di violazione dei dati (Data Breach)? (Sì/No)

Esito: **NON CONFORME (NO)**

Il personale è stato istruito su come riconoscere e segnalare immediatamente una sospetta violazione? (Sì/No)

Esito: **NON CONFORME (NO)**

6. Terze Parti (Responsabili Esterni)

Esiste un elenco di tutti i fornitori esterni (terze parti) che trattano dati per conto dell'azienda? (Sì/No)

Esito: **NON CONFORME (NO)**

Per ognuno di questi fornitori, è stato firmato un atto di nomina a "Responsabile del Trattamento" (Art. 28 GDPR)? (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda ha verificato che questi fornitori offrano garanzie di sicurezza e compliance adeguate? (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda sa se i suoi fornitori (es. servizi cloud, software) trasferiscono dati al di fuori dell'Unione Europea? (Sì/No)

Esito: **NON CONFORME (NO)**

Se sì alla precedente, sono state messe in atto le garanzie legali necessarie (es. Clausole Contrattuali Standard)? (Sì/No)

Esito: **NON CONFORME (NO)**

7. Privacy by Design e DPIA

Quando si avvia un nuovo progetto (o si acquista un nuovo software), si valuta l'impatto sulla privacy prima di iniziare? (Privacy by Design) (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda applica il principio di "minimizzazione" (raccoglie solo i dati strettamente necessari)? (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda adotta impostazioni di default che tutelano la privacy (es. caselle di consenso marketing non pre-spuntate)? (Privacy by Default) (Sì/No)

Esito: **NON CONFORME (NO)**

L'azienda ha valutato se svolge trattamenti a "rischio elevato" (es. monitoraggio dipendenti, dati sanitari su larga scala)? (Sì/No)

Esito: **NON CONFORME (NO)**

Se sì alla precedente, è stata condotta una Valutazione d'Impatto (DPIA)? (Sì/No)

Esito: **NON CONFORME (NO)**

Esiste una procedura per la distruzione sicura dei dati (cartacei e digitali) alla fine del periodo di conservazione? (Sì/N

Esito: **NON CONFORME (NO)**

_____

Firma del Responsabile