NOTIZIARIO

Sicur Book®

I.D.A.S.S.®
Indici Di Attenzione Sicurezza Salute

N°	Mese	Anno
5	maggio	2025

☞ **Argomento 1**

SICUREZZA SUL LAVORO E PROTEZIONE DATI DUE NORME A STRETTO CONTATTO DI APPLICAZIONE

La **protezione dei dati personali** è **strettamente connessa** alla **normativa sulla salute e sicurezza sul lavoro**: i due ambiti si integrano in modo significativo, perché la gestione della salute dei lavoratori **implica il trattamento di dati personali**, spesso **sensibili o appartenenti a categorie particolari** (es. dati sanitari, giudiziari, comportamentali).

pag.2

☞ **Argomento 2**

QUALI DOCUMENTI SONO NECESSARI ALL'APPLICAZIONE DEL GDPR ANCHE NEI CONFRONTI DEL D.LGS. 81/2008 E SMI

Per essere compliant al Regolamento UE 2016/679 (GDPR), ogni titolare del trattamento (impresa, ente, professionista, associazione) deve predisporre e mantenere una serie di documenti obbligatori, in base alla tipologia di trattamento effettuato, al rischio per i diritti e le libertà degli interessati e alla struttura organizzativa

Pag3

☞ **Argomento 3**

PROCEDURA INTEGRATA PROTEZIONE DEI DATI PERSONALI E SICUREZZA SUL LAVORO

Scopo della procedura è garantire che le attività aziendali legate alla salute e sicurezza sul lavoro siano svolte in conformità con il Regolamento (UE) 2016/679 (GDPR) estratto

Pag.7

CONNESSIONE GDPR 679/2016 E DLGS 81/2008

La **protezione dei dati personali** è parte integrante della **gestione della sicurezza sul lavoro**: ogni trattamento (es. sorveglianza sanitaria, monitoraggio comportamentale) deve essere svolto nel **rispetto dei principi del GDPR**, con misure specifiche per:

- riservatezza dei dati sanitari,
- separazione dei ruoli (es. medico vs. datore),
- collaborazione e coordinamento tra salute e sicurezza sul lavoro e protezione dati

Ecco una panoramica dettagliata:

---

1. Quadro normativo di riferimento

Regolamento UE 2016/679 (GDPR)

- Tutela i **dati personali dei lavoratori** in ogni fase del rapporto di lavoro.
- Richiede particolare attenzione per i **dati di salute** (art. 9 GDPR).

D.lgs. 81/2008 – Testo Unico Sicurezza sul Lavoro

- Impone obblighi al datore di lavoro in materia di **tutela della salute** dei lavoratori, anche attraverso visite mediche, sorveglianza sanitaria, giudizi di idoneità.
- Tali attività implicano la raccolta e gestione di **dati sensibili**.

---

2. Quando i due ambiti si intrecciano, esempio:

Situazione	Dati trattati	Rischio privacy
Visite mediche aziendali	Dati sanitari, anamnesi, giudizi d'idoneità	Obbligo di riservatezza e conservazione separata
Sorveglianza sanitaria lavoratori	Referti medici, indicazioni specialistiche	Accesso riservato solo al medico competente
Gestione infortuni sul lavoro	Certificati, cause, patologie	Obbligo di minimizzazione e protezione
Quasi incidenti - quasi infortuni	Analisi e valutazione delle cause - personale coinvolto	Obbligo di minimizzazione e protezione
Riunione annuale ex art.35 d.lgs. 81/2008 e smi	Dati salute ex art.9 GDPR 679	garantire che tali dati siano trattati nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, limitazione della conservazione e integrità e riservatezza.
Valutazione stress lavoro-correlato	Questionari, dati soggettivi	Anonimizzazione o pseudonimizzazione
Monitoraggio comportamenti o presenza (es. badge, GPS)	Dati di localizzazione e orari	Trasparenza, proporzionalità e informazione
Esercitazioni emergenza: evacuazione, antincendio, pronto soccorso	Partecipanti alle esercitazioni	Obbligo di riservatezza verbali

3. Principi GDPR applicabili alla sicurezza sul lavoro

✅ **Minimizzazione**

Trattare solo i dati strettamente necessari (es. non raccogliere diagnosi, ma solo il giudizio di idoneità).

✅ **Limitazione delle finalità**

Usare i dati solo per garantire la sicurezza, non per altri scopi (es. controllo disciplinare).

✅ **Riservatezza**

I documenti sanitari devono essere **gestiti solo dal medico competente**, **separati** da altri dati, e **non accessibili al datore di lavoro** se non nei limiti previsti.

✅ **Accountability**

Il datore di lavoro deve **dimostrare di avere adottato** misure tecniche e organizzative per proteggere i dati anche nel contesto della sicurezza.

❗ 4. Documenti e adempimenti comuni

Documento	Note
Registro trattamenti GDPR	Deve includere le attività legate alla sorveglianza sanitaria
Nomina medico competente come responsabile del trattamento	Se opera per conto del datore di lavoro per la sorveglianza sanitaria
Informative ai lavoratori	Su come vengono trattati i loro dati sanitari o comportamentali
Procedure aziendali di sicurezza	Devono prevedere misure privacy nei protocolli di gestione infortuni, stress, DPI…
Protezione documenti cartacei e digitali	Cartelle cliniche, giudizi di idoneità, riunioni annuali, registri visite devono essere protetti e conservati correttamente

❗ 5. Indicazioni del Garante Privacy

Il Garante ha ribadito più volte che:

- Il **datore di lavoro non può accedere ai dati di salute** se non nei limiti consentiti dalla legge.
- Il **medico competente** è tenuto a:
  - trattare i dati in modo riservato,
  - fornire solo giudizi sintetici (idoneità/non idoneità, con limitazioni),
  - conservare separatamente la documentazione sanitaria.

Le schede sanitarie e di rischio dei lavoratori sottoposti a sorveglianza sanitaria, devono essere conservate **in un luogo protetto** che garantisca:

- **riservatezza** (accesso solo da parte del medico competente o da soggetti da lui autorizzati o dal datore di lavoro o persona da lui autorizzata)
- **sicurezza fisica e informatica** (es. armadi chiusi a chiave o software criptati)
- **tracciabilità degli accessi**

Se conservate in formato digitale, devono essere **firmate digitalmente dal medico competente** e **protette da sistemi di sicurezza informatica adeguati** (es. backup, antivirus, autenticazione forte).

Se la cartella è cartacea, la stessa può essere conservata direttamente in azienda con salvaguardia del segreto professionale. Per poter dire di rispettare tale segreto il medico deve porre in essere tutte le misure che consentano effettivamente alla cartella di essere segreta, come:

- adottare buste sigillate dal medico;
- predisporre un archivio specifico al quale possa accedere solo il medico.

Rispetto del GDPR

Trattandosi di **dati sanitari**, rientrano nelle categorie particolari di dati personali (art. 9 GDPR). Pertanto:

- **il medico competente è titolare autonomo** del trattamento per quanto attiene alla sorveglianza sanitaria
- il datore di lavoro **non può accedere ai contenuti sanitari**, ma solo alle idoneità alla mansione (esito conclusivo)

Quali documenti sono obbligatori, raccomandati, di fatto necessari per adeguamento GDPR e DLGS 81

DOCUMENTI OBBLIGATORI AI SENSI DEL GDPR

1. Registro dei trattamenti (Art. 30 GDPR)

- **Obbligatorio** per aziende con +250 dipendenti o **se si trattano dati non occasionali** (***esempio dati di dipendenti, fornitori, archivio clienti…***) **sensibili** (***esempio: salute, infortuni, malattie professionali, sorveglianza sanitaria…***) **o giudiziari** (***esempio: prescrizioni organo vigilanza in caso di infortuni, inadempienze in materia di sicurezza sul lavoro…***).
- **Deve contenere**:
  - Finalità del trattamento
  - Categorie di interessati e dati
  - Destinatari dei dati
  - Tempi di conservazione
  - Misure tecniche e organizzative di sicurezza (Incident Response Plan - Data Breach…)
  - **Deve essere costantemente aggiornato riportando la data dell'ultimo aggiornamento**

Obbligatorio anche per fornitori (Responsabili esterni del trattamento) in forma distinta.

---

2. Informative privacy (Art. 13–14 GDPR)

- Fornite **a ogni interessato** al momento della raccolta dei dati, prima del consenso
- Devono essere **chiare e complete**, e includere:
  - Finalità e base giuridica
  - Titolare e contatti
  - Durata di conservazione
  - Diritti dell'interessato
  - Eventuali trasferimenti extra-UE

---

3. Consenso al trattamento (Art. 6 e 7 GDPR)

- Necessario **solo se la base giuridica del trattamento è il consenso** (es. marketing, profilazione, cookies non tecnici).
- Deve essere:
  - **Libero, informato, specifico e revocabile**
  - Documentato (es. modulo firmato: informativa+ consenso dettagliato)

---

4. Nomine ai Responsabili del trattamento (Art. 28)

- Ogni fornitore esterno che tratta dati per conto del titolare (es. commercialista, gestore cloud, software HR) deve essere **nominato formalmente responsabile**.
- La **nomina va fatta per iscritto** con atto che definisca:
  - Tipologia di dati
  - Finalità e limiti
  - Obblighi e misure di sicurezza

---

5. Nomine degli autorizzati al trattamento (Art. 29)

- I **dipendenti e collaboratori interni** devono essere **designati per iscritto** e **formati** in materia di trattamento dei dati personali
- Il documento deve specificare:

- Ruolo e ambito del trattamento
- Obbligo di riservatezza

---

6. Valutazione d'impatto sulla protezione dei dati (DPIA – Art. 35)

- Obbligatoria per trattamenti **ad alto rischio**, ad esempio:
  - Videosorveglianza sistematica su larga scala
  - Trattamenti automatizzati o profilazione
  - **Dati sanitari (sorveglianza sanitaria dei lavoratori d.lgs 81/2008 e smi) o biometrici**
- Include:
  - Analisi dei rischi
  - Misure di mitigazione
  - Verifica dell'impatto residuo

---

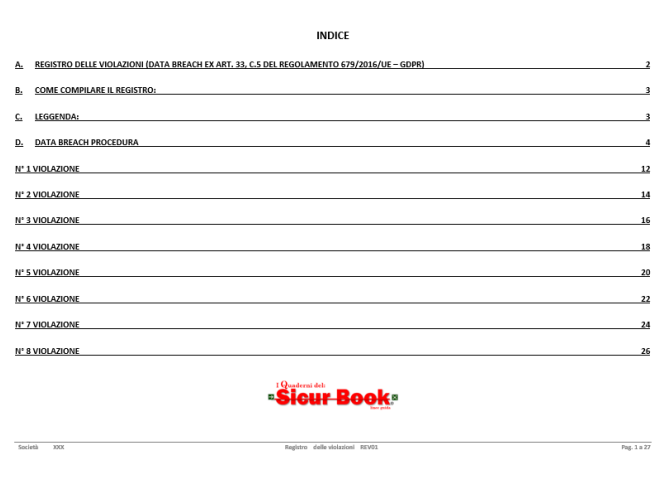
7. Politiche interne di sicurezza e procedure (Art. 24, 32)

- Documento (o manuale) che descriva:
  - Misure tecniche (es. backup, antivirus, crittografia)
  - Misure organizzative (formazione, controllo accessi)
  - Procedure in caso di violazione o data breach

---

8. Registro delle violazioni (data breach) (Art. 33)

- Obbligatorio **tenere traccia** di qualsiasi violazione, anche se non notificata al Garante.
- Deve indicare:
  - Data, natura, impatto stimato
  - Azioni correttive adottate
  - Eventuale notifica all'interessato



INDICE

---

9. Registro della formazione privacy - attestati partecipazione ai corsi

- Non richiesto espressamente, ma **essenziale** per dimostrare l'accountability.
- Attesta che il personale è stato:
  - Formato sui rischi e procedure GDPR
  - Aggiornato periodicamente
  - Allegati attestati di formazione ed eventuali aggiornamenti

---

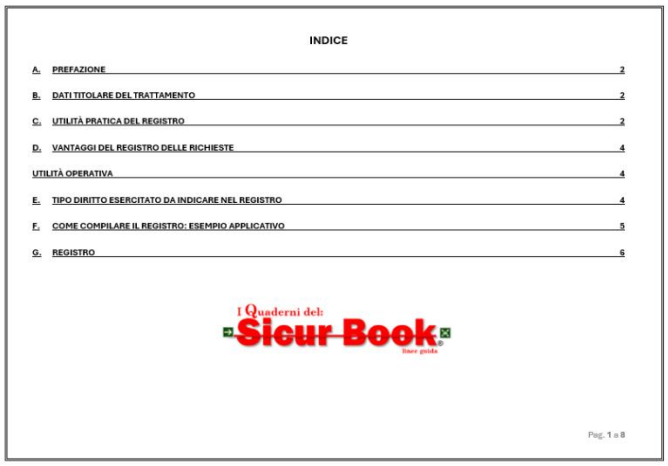
10. ALTRI DOCUMENTI RACCOMANDATI (ma non obbligatori)

☞ **Manuale GDPR aziendale o codice di condotta interno**

Il codice di condotta rappresenta uno strumento pratico per attuare i principi del GDPR (es. minimizzazione, integrità, riservatezza), aiutando l'organizzazione a dimostrare la propria accountability (art. 5, par. 2 e art. 24 GDPR).

☞ **Registro richieste interessati:**

Il **registro delle richieste da parte degli interessati** è **fortemente raccomandato** e può essere **decisivo ai fini della conformità al GDPR**, anche se **non esplicitamente obbligatorio**.



È un registro in cui si annotano tutte le **richieste formali o informali** avanzate dagli interessati in base agli **articoli da 15 a 22 del GDPR**, tra cui:

Articolo	**Diritto dell'interessato**
15	Accesso ai dati personali
16	Rettifica
17	Cancellazione (diritto all'oblio)
18	Limitazione del trattamento
20	Portabilità dei dati
21	Opposizione al trattamento
22	Esclusione da decisioni automatizzate

In quali casi è utile il registro: esempio richiesta copia attestati in materia di sicurezza sul lavoro corsi da parte di un dipendente

"Autorizzazione generale al trattamento dei dati sensibili nei rapporti di lavoro - n. 1/2000"

In particolare, questa autorizzazione include disposizioni sul trattamento dei dati relativi alla formazione professionale del lavoratore. Anche se non c'è un *esplicito obbligo normativo* in tale provvedimento che imponga al datore di lavoro di consegnare una copia degli attestati, **il principio sottostante è chiaro: il lavoratore ha diritto ad accedere ai propri dati personali, inclusi quelli relativi alla formazione.**

Questo diritto è poi stato confermato e rafforzato dal successivo:

📘 Regolamento (UE) 2016/679 (GDPR) – art. 15

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento*. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune….*

riconosce a ogni interessato il diritto di ottenere una copia dei dati personali trattati, tra cui rientrano senz'altro gli attestati di formazione rilasciati nel contesto del rapporto di lavoro.

☞ **Il datore di lavoro è tenuto a consegnare copia degli attestati di formazione** se il dipendente ne fa richiesta, **in virtù del diritto di accesso ai dati personali** (oggi disciplinato dall'art. 15 GDPR).

La **delibera del 7 marzo 2000** costituiva un primo passo in questa direzione, oggi superato dal GDPR ma utile come riferimento storico.

Il registro, nella Sua interezza,

- **Dimostra l'accountability**: si dà evidenza che sono stati gestiti correttamente i diritti degli interessati.
- **Evita sanzioni**: se il Garante chiede conto di una richiesta, è fondamentale poterlo dimostrare.
- **Rispetta i termini**: il GDPR impone di rispondere entro **30 giorni**, quindi serve una tracciabilità.
- **Aiuta nella gestione dei reclami o contenziosi**: una richiesta documentata Vi tutela.

Il registro come, tutti gli altri documenti, sono riservati ai clienti con contratto di assistenza o che hanno richiesto l'adeguamento al GDPR 679/2016.

PROCEDURA INTEGRATA PROTEZIONE DEI DATI PERSONALI E SICUREZZA SUL LAVORO

La procedura si applica a tutti i trattamenti di dati personali effettuati nell'ambito delle attività di sorveglianza sanitaria, visite mediche, gestione degli infortuni, valutazione dei rischi e formazione obbligatoria ai sensi del D.Lgs. 81/2008.

Esempio:

❗ Ruoli e responsabilità:

- Il Titolare del trattamento: garantisce la compliance al GDPR e al D.lgs. 81/2008.
- Il Medico competente: gestisce i dati sanitari dei lavoratori come autonomo titolare o responsabile nominato.
- Il RSPP e il personale HR: gestiscono documentazione di sicurezza nel rispetto dei principi GDPR.
- I lavoratori: devono essere informati e formati sul trattamento dei propri dati personali.

❗ Principi di trattamento (GDPR)

- Liceità, correttezza e trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza e aggiornamento
- Limitazione della conservazione
- Integrità, riservatezza e responsabilizzazione

❗ Nomine e informative

- Nomina del medico competente come responsabile del trattamento (se applicabile)
- Informativa specifica ai lavoratori sul trattamento dei dati sanitari
- Nomina dei dipendenti autorizzati al trattamento con istruzioni scritte

❗ Formazione e consapevolezza

Il personale dipendente è formato periodicamente su:
- Protezione dei dati personali
- Gestione della documentazione sanitaria
- Riservatezza e sicurezza informatica

☞ **Informativa Protezione dati personali**

Spett.le Cliente, riceve la presente newsletter, sotto forma di notiziario SICURBOOK®, quale informativa specifica in materia di sicurezza sul lavoro e protezione dati personali, in quanto cliente che ha usufruito e/o usufruisce dei nostri servizi in materia di sicurezza sul lavoro e/o protezione dati personali; se non desidera più ricevere il presente notiziario, potrà disdirlo in qualunque momento, inviando una comunicazione via email come quella indicata a fondo pagina.

Se desidera ricevere informazioni in merito sui servizi da noi erogati, o in merito a quanto indicato nel presente notiziario dai propri collaboratori, Le chiediamo cortesemente di compilare il format sotto riportato e inviarlo a info@sicurezzascs.it:

Tipo Richiesta		Informazioni relative a:

Persona che richiede informazioni:

Nome	
Cognome	
Ruolo	
Telefono	
Indirizzo	
Cap	
Città	
Provincia	

Questo documento è inviato esclusivamente per il destinatario. Tutte le informazioni ivi contenute, compresi eventuali allegati, sono soggette a riservatezza a termini del vigente GDPR 679/2016 in materia di protezione dei dati personali e quindi ne è proibita l'utilizzazione. Se avete ricevuto per errore questa newsletter, Vi preghiamo cortesemente di contattare immediatamente il mittente e cancellare la e-mail dandocene immediata comunicazione, utilizzando il fac simile sotto riportato.
Informativa privacy art. 13 Regolamento UE n. 2016/679: Titolare del trattamento dei dati è SCS SICUREZZA SRL UNIPERSONALE con sede Via Sestri, 3/3 – 16154 Genova.
Sito internet www.sicurezzascs.it tel 010.37762.92 - Contitolare Trattamento Roberto Ferro - Contitolare Trattamento CSA Centro Sicurezza Applicata di Alessandro Ferro & C. sas
Per cancellarti dal ricevere le newsletter di SICURBOOK invia Email a info@sicurezzascs.it unito ad un documento di riconoscimento della persona autorizzata (vedi anche sito Garante della privacy)
Garanzia di riservatezza e tutela della privacy **GDPR 679/2016**
Per cancellare o modificare gli argomenti di tuo interesse delle newsletter di SICURBOOK NEWS invia la presente:

☞ **Richiesta Cancellazione invio via email del SICURBOOK a: info@sicurezzascs.it**

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

Il Sottoscritto: _____in qualità di _____
dell'azienda_____
con sede:_____email_____

richiede la cancellazione dell'invio di newsletter quale il notiziario SICURBOOK con effetto immediato
data___/____/_____ firma avente diritto richiesta

_____

[1]Allegare copia di un documento di riconoscimento

☞ Per informazioni:

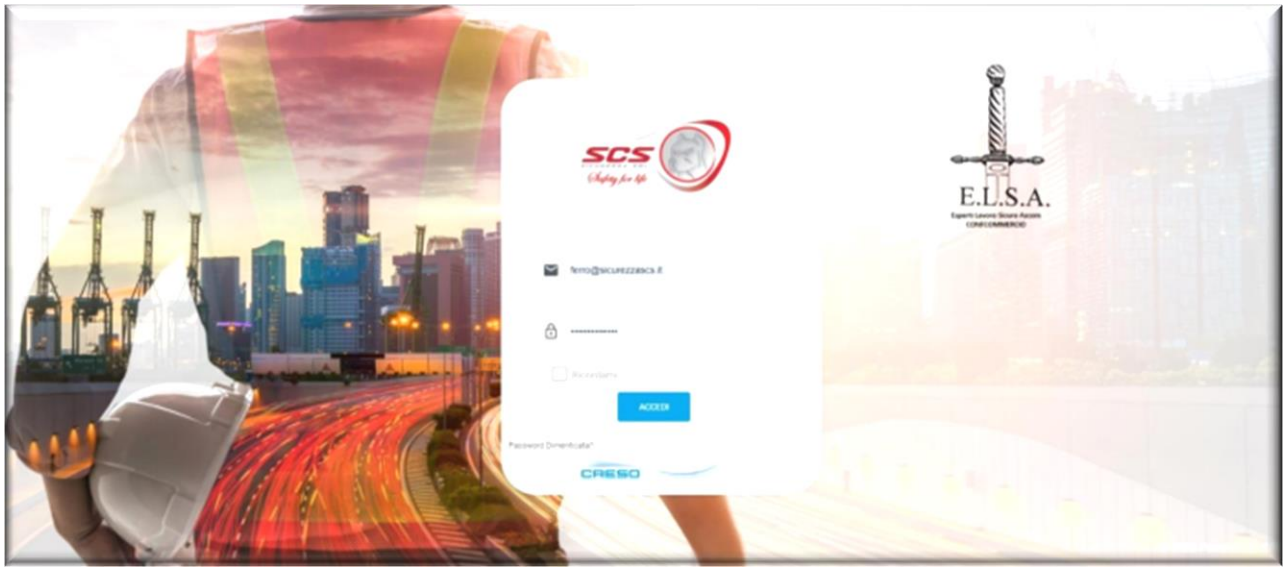
SCS SICUREZZA srl Unipersonale	Via Sestri 3/3 Genova tel.010.377.62.92 p.i. 01574270995	info@sicurezzascs.it web:www.scssicurezza.it
C.T.P. Roberto Ferro **Iscritto Albo Consulenti Tecnici Tribunale di Genova dal 1998** **Sicurezza sul lavoro ex d.lgs. 81/2008** **D.P.O.** **ex GDPR 679/2016**	Tel:348.31.27.720	ferro@sicurezzascs.it info@sicurezzascs.it

In collaborazione con:

Avvocato Tommaso Ferro Consulenza legale e formazione	Tel:347.14.20.113	avvtommasoferro@gmail.com

In collaborazione con:

CSA CENTRO SICUREZZA APPLICATA	Via delle Primule 101 16148 Genova Tel. 010.0899266/345	ufficio@csasicurezza.it
Dott. Alessandro Ferro	Tel:010.0899266/345	ufficio@csasicurezza.it
Dott.ssa Irene Carella	Tel:010.0899266/345	ufficio@csasicurezza.it
Dott. Nicolò Ferro	Tel:010.0899266/345	ufficio@csasicurezza.it



Sicur Book®

Il Sistema di gestione sicurezza *è online*!!!!