Notiziario Sicurezza & Privacy

Aggiornamenti, linee guida e approfondimenti tecnici per imprese e professionisti

SicurBook®

E.L.S.A.
Esperti Lavoro Sicuro Ascom
CONFCOMMERCIO

N°	Mese	Anno
03	Maggio	2026

Scansiona QR code per visitare il nostro sito
www.scssicurezza.it

Argomento 1

Accordo Stato-Regioni 2025: scade il periodo transitorio

Dal 19 maggio 2026 non sarà più possibile erogare corsi secondo i vecchi accordi sulla formazione in materia di salute e sicurezza sul lavoro.
Un approfondimento su scadenze, aggiornamenti obbligatori e adeguamenti richiesti alle aziende.

Approfondimento a pag.2

Argomento 2

Posta elettronica aziendale dei dipendenti: il Garante Privacy declina le regole del gioco. Cosa devono fare le imprese italiane.

Con il Provvedimento n. 165 del 12 marzo 2026 (pubblicato nella Newsletter del 15 aprile 2026), il Garante per la Protezione dei Dati Personali ha tracciato un orientamento destinato a diventare il nuovo standard nazionale su privacy, posta elettronica e rapporti di lavoro.

Una compagnia assicurativa è stata sanzionata con 50.000 euro per non aver garantito l'accesso integrale alle email dell'ex dipendente e per aver conservato in modo non conforme i contenuti e i log di navigazione. **a pag.3**

ACCORDO STATO REGIONI

L'Accordo Unico Stato-Regioni sulla formazione in materia di salute e sicurezza sul lavoro, come precedentemente comunicato, ha riorganizzato l'intero sistema formativo, introducendo un testo unico che accorpa e sostituisce i precedenti accordi (2011-2012 e 2016).

Le novità principali per le figure presenti nell'organizzazione della sicurezza aziendale:

- **Datore di Lavoro:** È introdotto l'obbligo di un corso di formazione di 16 ore (con un modulo integrativo di 6 ore per i cantieri), oltre a un aggiornamento quinquennale di 6 ore. I datori di lavoro hanno tempo per mettersi in regola fino al 23 maggio 2027.
- **Preposti:** L'aggiornamento è ora obbligatorio con cadenza **biennale** (minimo 6 ore) e non più quinquennale.
- **Lavoratori, RSPP, ASPP:** La formazione per i lavoratori prevede un test di apprendimento obbligatorio, mentre per RSPP e ASPP l'aggiornamento resta quinquennale.

Come specificato in precedenza, non sono state apportate modifiche alle durate e alla periodicità di aggiornamento, **l'unica vera modifica di rilievo è stata eliminata la frase riportata nel vecchio accordo del 2011, che concedeva la possibilità di completare la formazione dei lavoratori entro 60 giorni dall'assunzione, ma solo in prima applicazione dell'accordo stesso, e non poche realtà, recentemente si sono viste sanzionare per una mancata o troppo tardiva applicazione dell'art 37 ovvero per la mancata formazione dei lavoratori..** infatti tale frase, tempo 60 gg, aveva generato diverse interpretazioni non corrette, in ogni caso, a scanso di ulteriori equivoci, tale "possibilità" è stata cancellata e quindi, secondo il legislatore, la formazione deve essere effettuata prima di adibire il lavoratore all'attività lavorativa.

- Risulta evidente che per molte aziende il rispetto di tale disposizione sia a dir poco "complicato", occorrerà potenziare le misure compensative (informazione/addestramento) proprio perché in alcuni casi sarà impossibile formare i lavoratori prima di adibirli all'attività lavorativa.

Riconoscimento della formazione pregressa:

- Tutti i corsi effettuati in vigenza del vecchio accordo sono riconosciuti, i lavoratori dovranno effettuare l'**aggiornamento** mantenendo la vecchia periodicità (5 anni), tranne per il settore edile 3 anni.

- **Corso Preposti**

È una delle **figure che ha subito i cambiamenti maggiori**.

- Nuova durata corso base: 12 ore
- Nuova periodicità di aggiornamento: 2 anni
- Durata corso di aggiornamento: 6 ore (non cambia rispetto al precedente accordo)

- **Corso Datore di Lavoro Non RSPP**

Tale corso nei precedenti accordi non era previsto, questo significa che i **datori di lavoro di ogni azienda**, che non ricoprono il ruolo di RSPP, **dovranno frequentare un corso di formazione come di seguito dettagliato**:

- Corso base: durata 16 ore
- Per il settore edile, i datori di lavoro delle imprese affidatarie, dovranno frequentare il modulo aggiuntivo "cantieri" della durata di 6 ore, questo permetterà di adempiere a quanto previsto dall'art. 97 del D. Lgs. 81/08 (obblighi di vigilanza delle imprese affidatarie in cantiere)
- Corso aggiornamento: durata 6 ore
- Periodicità: ogni 5 anni

Proprio per il fatto che l'obbligo di formazione è stato introdotto con il nuovo accordo, i datori di lavoro che non hanno mai effettuato corsi, avranno tempo **24 mesi per svolgere la formazione**, ovvero entro il 24/05/2027.

Riconoscimento della formazione pregressa:

I corsi di formazione già erogati alla data di entrata in vigore del presente accordo, i cui contenuti siano conformi al nuovo accordo sono riconosciuti. L'aggiornamento (5 anni) dei suddetti corsi parte dalla data di fine corso riportata nell'attestato.

- **Addetti all'Utilizzo di Attrezzature che richiedono Specifica Abilitazione**

In questo caso **non cambiano le durate e le periodicità delle varie attrezzature citate nei precedenti accordi,** le novità riguardano l'introduzione di alcune attrezzature che non erano presenti nel vecchio accordo.

Posta aziendale (fonte Garante Privacy)

Proprietà dello strumento e titolarità dei dati. Anche se l'account di posta è aziendale, il suo contenuto (compresa la corrispondenza "lavorativa") resta dato personale del lavoratore.

Diritto di accesso ex artt. 12 e 15 GDPR: integrale e senza filtri preventivi. Alla cessazione del rapporto (o su richiesta formale), l'ex dipendente ha diritto ad accedere a tutta la casella di posta ancora nella disponibilità dell'azienda, inclusi i backup. Non sono più ammessi filtri discrezionali tra "email personali" e "email lavorative". Solo nel caso di un segreto aziendale, il know-how possono giustificare limitazioni (art. 15 par. 4 GDPR), ma solo se motivate caso per caso, proporzionate, documentate e tali da dimostrare un pregiudizio serio e concreto. Non sono ammessi gli oscuramenti generalizzati "a monte".

Inoltre è opportuno richiamare il costante orientamento della Corte europea dei diritti dell'uomo che, in alcune pronunce (richiamate anche nei provvedimenti dell'Autorità), ha osservato come la linea di confine tra ambito lavorativo/professionale e ambito strettamente privato non sempre può essere tracciata con chiarezza, motivo per cui deve ritenersi applicabile, anche all'ambito lavorativo, l'art. 8 della CEDU posto a tutela della vita privata.

Anche le comunicazioni di tipo elettronico scambiate sul luogo di lavoro rientrano, quindi, nelle nozioni di "vita privata" e di "corrispondenza", di cui al citato articolo 8 (si vedano le pronunce Niemietz c. Allemagne, 16/12/1992 (ric. n. 13710/88), spec. par. 29; Copland v. UK, 03/04/2007 (ric. n. 62617/00), spec. par. 41; Bărbulescu v. Romania [GC], 05/09/2017 (ric. n. 61496/08), spec. par. 70-73; Antović and Mirković v. Montenegro, 28/11/2017 (ric. n. 70838/13), spec. par. 41-42).

La protezione della vita privata si estende, dunque, anche all'ambito lavorativo, considerato che, proprio in occasione dello svolgimento di attività lavorative e/o professionali, si sviluppano relazioni dove si esplica la personalità del lavoratore (v. artt. 2 e 41, comma 2, Cost.).

Pertanto, il trattamento dei dati, effettuato mediante tecnologie informatiche, nell'ambito del rapporto di lavoro, deve conformarsi al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, a tutela di lavoratori e di terzi (v. Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, spec. punto 3).

Coerentemente con questa impostazione, nel provvedimento recante "Linee guida per posta elettronica e Internet" l'Autorità ha osservato che "Il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati – riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali" (provvedimento del 01/03/2007, n. 13, doc. web n. 1387522, punto 5.2, lett. b). Orientamento che è stato ribadito anche in provvedimenti adottati dall'Autorità nell'ambito di specifiche istruttorie su casi concreti (si vedano provv.ti: n. 8 del 16/01/2025, doc web n. 10110927; n. 732 del 27/11/2024, doc web n. 10101221; n. 353 del 29/09/2021, doc web n. 9719914).

Alla luce di quanto sopra, deve quindi ritenersi contraria ai principi in materia di protezione dei dati personali la condotta, posta in essere dalla Società, consistente nella decisione di esaminare preventivamente il contenuto delle e-mail presenti sull'account di posta elettronica individualizzato dell'interessato, al fine di limitare l'accesso dello stesso alle sole comunicazioni di carattere "strettamente personale", sull'erroneo convincimento che lo scambio di corrispondenza, intrattenuto sull'account aziendale, sia di piena ed esclusiva disponibilità dell'azienda.

Su questo aspetto, infatti, alla luce delle definizioni di “dato personale” e “trattamento”, di cui all’art. 4, n. 1 e 2, del Regolamento, che ricomprendono necessariamente anche i dati relativi all’attività lavorativa, le comunicazioni in transito su un account individualizzato sono inevitabilmente riconducibili a dati personali dell’assegnatario dell’account.

Deve ritenersi illecita peraltro anche l’ulteriore attività di oscuramento e anonimizzazione effettuata dalla Società sul contenuto della corrispondenza del reclamante, per rispondere all’esigenza di tutelare i diritti dei terzi e i segreti aziendali contenuti nelle e-mail.

Infatti, viste le ipotesi tassativamente previste dal Regolamento in cui il diritto di accesso può essere limitato solo in caso di richieste manifestamente infondate o eccessive (art. 12, par. 5, del Regolamento) e di tutela dei diritti dei terzi (art. 15, par. 4, del Regolamento), si rileva come nel caso di specie non ricorra nessuna delle circostanze previste dalla norma.

In particolare, per quel che riguarda la tutela dei diritti e delle libertà altrui, il considerando 63 precisa che tra questi va compreso anche il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d’autore che tutelano il software.

…

Nell’ambito dell’istruttoria svolta, è emerso che la Società effettua una conservazione delle e-mail che transitano sugli account aziendali dei propri dipendenti, mediante un backup della posta elettronica disposta per un periodo di cinque anni, al fine di “preservare il patrimonio informativo della società in relazione all’attività di vigilanza a cui la stessa è sottoposta” (nota del 02/05/2024 e meglio specificato nelle memorie difensive del 24/09/2024).

Occorre innanzitutto osservare che la specifica attività di backup, disposta dalla Società sul contenuto delle caselle di posta elettronica assegnate ai dipendenti, non è stata contemplata e disciplinata in nessuno dei documenti informativi predisposti nei confronti dei dipendenti.

Trasparenza assoluta tra informative, policy e prassi. Qualsiasi difformità tra ciò che si scrive e ciò che si fa viola i principi di correttezza e trasparenza del GDPR e rischia di invalidare provvedimenti disciplinari.

La violazione accertata nei termini di cui in motivazione non può essere considerata “minore”, tenuto conto della natura delle plurime violazioni accertate, che hanno riguardato i principi generali del trattamento dei dati e le disposizioni più specifiche in materia di controlli a distanza, della gravità e della durata della violazione stessa, del grado di responsabilità e della maniera in cui l'autorità di controllo ha preso conoscenza della violazione (v. Considerando 148 del Regolamento).

Visti i poteri correttivi attribuiti dall’art. 58, par. 2, del Regolamento, alla luce delle circostanze del caso concreto, si dispone di:

- consentire al reclamante l’accesso integrale al contenuto della corrispondenza presente sull’account di posta elettronica aziendale, di tipo individualizzato, utilizzato nel corso del rapporto di lavoro;

- conformare le policy aziendale e i trattamenti descritti alla disciplina in materia di protezione dei dati personali come richiamata nei par. 3.2 e 3.3;

- l’applicazione di una sanzione amministrativa pecuniaria ai sensi dell’art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i), del Regolamento).

Spett.le Cliente,
riceve la presente newsletter, sotto forma di notiziario SICUR BOOK®, 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. scssicurezza.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 SICUR BOOK NEWS invia la presente:

☞ **Richiesta Cancellazione invio via email del SICUR BOOK 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:

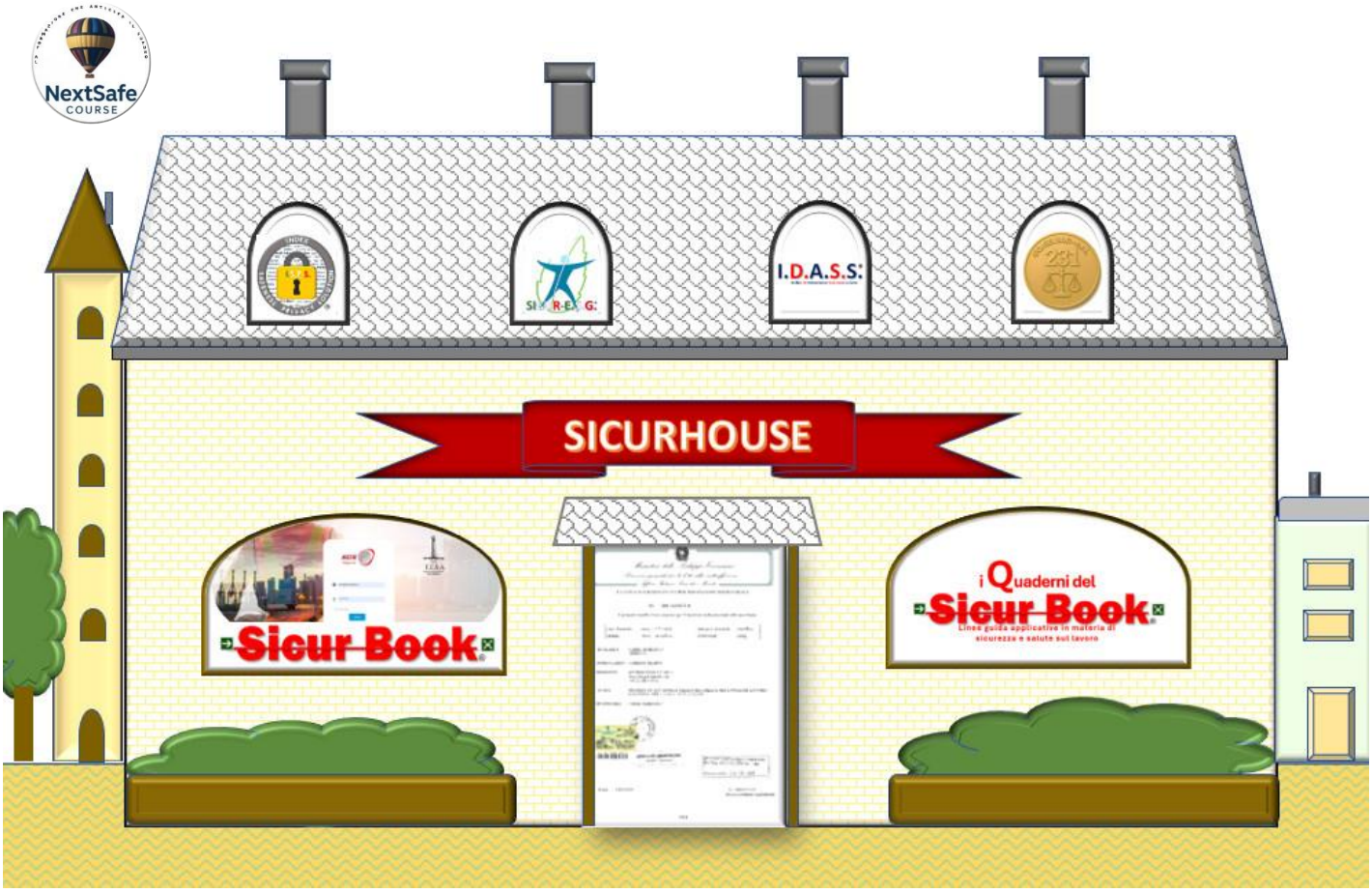
SCS SICUREZZA srl Unipersonale	Via Sestri 3/3 Genova tel.010.377.62.92 p.i. 01574270995	info@sicurezzascs.it web:www.scssicurezza.it
C.T.P. Roberto Ferro **Sicurezza sul lavoro - CTP** **DPO - GDPR 679/2016**	Tel:348.31.27.720	ferro@sicurezzascs.it info@sicurezzascs.it

In collaborazione con:

Avv. **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



www.scssicurezza.it