Rinnovo 30 marzo 2018 - **Personale non medico dipendente da case di cura private laiche e religiose e da centri di riabilitazione** *(sottoscritto da CIU, ESAARCO, CEPA-A, ESAARCO Sanità, ESAARCO Federcoop, SAI, ESAARCO FER e UGL, FISNAL CTA, FENAL Sanità, SI-CEL, CLI CIU, FNAOPS CLI CIU, ONAPS)*

1. *Servizi degli istituti contrattuali* - Le parti sociali di cui sopra per il presente ccnl hanno convenuto che i servizi erogati dagli istituti contrattuali (Enti Bilaterali, Organismi Paritetici, Fondi Interprofessionali, ecc.) comportano l'erogazione degli stessi a propri associati, verranno pertanto rilasciati servizi computando l'importo del servizio stesso compresa la quota associativa per l'azienda e per i lavoratori dipendenti della stessa, lo status di associato verrà mantenuto fino all'annualità di fruizione del servizio terminata la quale decadrà lo status di associato salvo che non venga erogato da parte di uno degli istituti contrattuali altro servizio, in quel caso lo status di associato si intenderà rinnovato per un'altra annualità.

2. *Privacy* -
GDPR "General Data Protection Regulation"

Il nuovo Codice della privacy in materia di diffusione dei dati personali, voluto fortemente da tutti gli Stati Membri dell'Unione Europea. sostituirà in pieno il codice del 1995 e il successivo codice in materia di protezione dei dati personali del 2003.

Nell'aprile 2016 è animata l'adozione del testo da parte del Consiglio Europeo e del Parlamento europeo, e il 4 maggio 2016, i testi del Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola il trattamento dei dati personali sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea. Il Regolamento è in vigore 20 giorni dopo la pubblicazione in Gazzetta e sarà elettivamente applicabile in tutti gli Stati Membri, Italia inclusa, dal 25 maggio 2018: è questa la data stabilita per tutti i paesi. In quel giorno, infatti, dovrà essere garantito il perfetto allineamento delle varie normative nazionali con le disposizioni previste dal Regolamento.

Il nuovo regolamento contiene una serie di importanti novità soprattutto per le aziende.

È deciso, infatti, che l'Autorità di vigilanza europea riguarderà anche le imprese con sede estera e operanti nell'Unione Europea.

Il Regolamento introduce il "diritto all'oblio", regolamentato dall'art. 17: "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste albo fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Per quanto riguarda le aziende, l'art. 5 del GDPR 2018 prevede una serie di principi validi per il trattamento dei dati, incluso quello della "responsabilizzazione" che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, tutti gli altri principi. In questo senso, dunque, le amministrazioni, così come suggerito dal Garante per la protezione dei dati personali, dovranno dotarsi di un Responsabile della protezione dei dati, di un Registro delle attività di trattamento e prepararsi alla notifica delle violazioni dei dati personali.

Il Regolamento Generale sulla Protezione dei Dati (GDPR 2018) stabilisce le nuove regole per trattare i Dati Personali all'interno della Comunità Europea e disciplinare l'esportazione dei Dati Personali al di fuori dei confini UE.

Il Regolamento UE 2016/679 (General Data Protection Regulation) si applica non solo ai cittadini dell'Unione Europea ma anche agli Enti che risiedono al di fuori dei Paesi membri.

Nel nuovo Regolamento GDPR/18 si definisce Dato Personale "qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale che pubblica come nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di socialnetwork, informazioni mediche o indirizzi IP di computer".

Il nuovo Regolamento descrive in che maniera i dati personali vadano protetti ("data protection") e trattati in conformità con le normative vigenti. La sicurezza informatica (ICT-SEC) nel nuovo Regolamento Europeo per la Protezione dei Dati verrà presa in considerazione per il Trattamento e la Protezione dei Dati Personali. Nuovi principi vengono introdotti dal General Data Protection Regulation: i dati vanno trattati seguendo nuovi principi di applicazione, e il trattamento deve seguire un ciclo progettato, riconosciuto come "trattamento by design''. I diritti degli interessati devono essere gestibili in qualunque fase del ciclo di trattamento dei Dati Personali su Internet e nei sistemi informatici: il Diritto alla Cancellazione del Dato Personale, il Diritto all'Oblio del Dato Personale sui motori di ricerca su Internet, e il Diritto al Blocco del Trattamento del Dato Personale. Vengono introdotti nuovi obblighi, come il SPIA - Data Protection

Impact Assesment, che prevede il monitoraggio sistematico del Trattamento dei Dati Personali sensibili e ad alto rischio.

Attraverso processi agevolati di certificazioni GDPR READY, e l'acquisizione di "bollini" che garantiscono la correttezza del Trattamento dei Dati, i Garanti Europei riconosceranno l'azienda o l'ente pubblico come conformi al nuovo Regolamento GDPR.

Tre i punti principali di cambiamento:

- la "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" (o anche conosciuta come Data Protection by Design and by Default). L'art. 25 GDPR, infatti, illustra il principio Privacy by Design e by Default, in quanto obbligo generale e prescrive: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", il titolare del trattamento "mette in atto misure tecniche e organizzative adeguate, quali la pseudominizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati". Nell'ambito della Privacy by Design e by Default, dunque, il titolare del trattamento deve assicurarsi di mettere in atto "misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento".

Tra le numerose novità introdotte dal regolamento, poi, c'è il principio di "responsabilizzazione", che diventerà centrale per aziende e pubbliche amministrazioni. Secondo il Principio dell'Accountability (o principio di responsabilizzazione), i titolari del trattamento dovranno sempre assicurare il rispetto dei principi applicabili al trattamento dei dati personali. "Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche", si legge nel preambolo del GDPR. Per questo motivo "non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche".

Il nuovo regolamento, all'art. 28 (Responsabile del trattamento) prevede che "Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato" e che "Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche".

Viene istituita, così, la figura del sub-responsabile. Se il responsabile del trattamento è scelto direttamente dal titolare del trattamento, che possiede tutta una serie di poteri, è possibile che la responsabilità venga, poi, ripartita, anche se rimane "l'opportunità di opporsi". Il responsabile, designato dal titolare, dunque, dovrà sempre informare il titolare stesso di eventuali modifiche. Si tratta, comunque, dell'unico caso in cui il responsabile ha una certa titolarità. In generale anche il sub-responsabile avrà gli stessi obblighi e lo stesso rapporto di subordinazione del responsabile, e opererà per conto del titolare.

Datore di lavoro e suoi "poteri" nei confronti dei dipendenti in tema di privacy

Oggi, attraverso i socialnetwork e i blog è sempre più facile "spiare" gli altri e capita sempre più spesso che le aziende, in vista di un colloquio o di un'assunzione, monitorino il profilo del candidato. Capita, inoltre, che le aziende utilizzino basi o post pubblicati sui social per scopi interni, come un ammonimento o addirittura il licenziamento. Ecco perché i Garanti europei della privacy si sono chiesti fino a dove può spingersi un datore di lavoro, nello "spiare" i propri dipendenti. L'importante è distinguere, sempre e comunque, l'ambito professionale da quello privato. Se si sospettano fughe di dati, ad esempio, si possono spiare, ma parzialmente, le comunicazioni dei dipendenti (la mail aziendale per intenderci). Si possono consultare, inoltre, i profili professionali degli stessi e permettere che usufruiscano di un cloud aziendale per il proprio lavoro.

I Garanti europei della privacy, inoltre, hanno evidenziato che l'azienda non può controllare indistintamente i profili social dei dipendenti. Prima dell'assunzione il controllo, nei limiti professionali, è legittimo così come il monitoraggio del profilo social solo per le informazioni pubblicamente reperibili. Ad assunzione avvenuta, invece, il controllo consentito è molto più limitato ed è legittimo solo se necessario per proteggere gli interessi dell'azienda stessa. Questo perché ciascun lavoratore - ricordano i Garanti - qualsiasi sia il contratto stipulato, ha diritto al rispetto della propria vita privata, della libertà e della dignità e dovrà, prima di tutto, essere informato sulla modalità di trattamento dei dati personali e sulle eventuali norme di controllo previste dall'azienda, dalla mail al cellulare aziendale.

Le mail private del lavoratore, invece, non possono mai essere spiate, mentre è consentita l'analisi del traffico, per ridurre, ad esempio, i rischi di attacco informatico. Sempre meglio utilizzare strumenti e misure preventive e trasparenti, che consentano ai dipendenti di capire cosa fare e non fare per il bene della società. L'ideale - concludono i Garanti - è che l'azienda si doti di connessioni WIFI dedicate, spazi ad hoc su computer e smartphone, su cloud e posta elettronica, non accessibili al datore di lavoro se non in casi eccezionali.

L'art. 37 del testo, infine, specifica la designazione del DPO (Data Protection Officer) e il responsabile della protezione dei dati. In ciascun settore, dunque, il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati quando "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala" e quando "le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali".

Le parti sociali mettono a disposizione di tutti i propri associati un percorso per venire in assistenza a coloro che hanno bisogno di formare il responsabile del trattamento dei dati interno o di ingaggiare un Data Protection Officer esterno e per porsi quale Ente che metta a norma l'azienda o l'attività commerciale in linea con le nuove normative vigenti sulla Privacy.

Il corso per responsabile trattamento dati interno

Il corso è di 20 ore in modalità e-learning.

Con il superamento del test online si otterrà l'attestato certificato dalla Commissione presieduta dall'ESAARCO socio CIELS con il percorso formativo validato dalla 11° sottocommissione Privacy dell'Istituto ad Ordinamento Universitario con D.M. 31 marzo 2010 SGML CIELS.

Il corso per responsabile trattamento dati esterno

Il corso è di 40 ore.

32 ore sono in modalità e-learning superate le quali si accede alle 8 ore finali in aula.

Nella giornata finale del corso si tiene la prova d'esame per l'ottenimento dell'attestato certificato dalla Commissione presieduta dall'ESAARCO socio CIELS con il percorso formativo validato dalla 11° sottocommissione Privacy dell'Istituto ad Ordinamento Universitario con D.M. 31 marzo 2010 SGML CIELS.

Il corso per DPO interno

Il corso è di 40 ore.

32 ore sono in modalità e-learning superate le quali si accede alle 8 ore finali in aula.

Nella giornata finale del corso si tiene la prova d'esame per l'ottenimento dell'attestato certificato dalla Commissione presieduta dall'ESAARCO socio CIELS con il percorso formativo validato dalla 11° sottocommissione Privacy dell'Istituto ad Ordinamento Universitario con D.M. 31 marzo 2010 SGML CIELS e da un Organismo di Certificazione accreditato Accredia.

Il corso per DPO esterno

Il corso è di 80 ore.

56 ore sono in modalità e-learning superate le quali si accede alle 24 ore finali in aula.

Nella giornata finale del corso si tiene la prova d'esame per l'ottenimento dell'attestato certificato dalla Commissione presieduta dall'ESAARCO socio CIELS con il percorso formativo validato dalla 11° sottocommissione Privacy dell'Istituto ad Ordinamento Universitario con D.M. 31 marzo 2010 SGML CIELS e da un Organismo di Certificazione accreditato Accredia.

Il corso formazione per formatori- privacy

Il corso è di 40 ore in modalità aula.

Nella giornata finale del corso si terrà la prova d'esame per l'ottenimento dell'attestato certificato dalla Commissione presieduta dall'ESAARCO socio CIELS con il percorso formativo validato dalla 11° sottocommissione Privacy dell'Istituto ad Ordinamento Universitario con D.M. 31 marzo 2010 SGML CIELS.

3. *Adeguamento tabelle economiche* - Le parti sociali concordano che entro 12 mesi dalla sottoscrizione del presente ccnl presenteranno l'adeguamento delle tabelle economiche, fin da adesso verrà creato un apposito tavolo di lavoro per procedere a tale adeguamento.

4. *Organismo Paritetico* - Le parti sociali in ottemperamento di quanto stabilito dagli Accordi Stato-Regioni, decidono di procedere con l'applicazione della norma per tutti i loro ccnl attraverso l'Organismo Paritetico Nazionale EFEI Italia in sigla OPN EFEI ITALIA, precedentemente costituito e formato dalle parti sociali maggiormente rappresentative comparativamente quali UGL e CIU (entrambi hanno un membro nel CNEL) da tutti gli Enti Bilaterali di emanazione dei ccnl previsti dal Protocollo di Accordo Interconfederale del 17 febbraio 2018 che ne nominano i membri delle aree di settore relativamente allo loro competenza, demandando a quest'ultimo tutti gli oneri relativi alla salute e sicurezza nei luoghi di lavoro.

5. *Commissione ccnl Lavoro e Sicurezza dell'Istituto ad Ordinamento Universitario CIELS* - Le parti sociali firmatarie del presente Protocollo Integrativo e Rinnovo contrattuale, tramite la Confederazione ESAARCO, socio dell'Istituto ad Ordinamento Universitario CIELS di Padova con D.M. 30 marzo 2010 hanno deciso di delegare alla "Commissione ccnl Lavoro e Sicurezza" la validazione dei percorsi formativi in tema di contenuti didattici conformi alla norma. La conformità degli stessi viene certificata attraverso l'apposizione del logo della Commissione e della firma in calce del Presidente della stessa.

La Commissione è costituita da undici (11) sottocommissioni, una per ognuno dei nove macro settori ATECO, una

sottocommissione per la Privacy ed una Sottocommissione per le Discipline Bio Naturali.

Ad ogni sottocommissione sono nominati tecnici esperti di settore dagli Enti Bilaterali composti dalle parti sociali firmatarie del presente Protocollo Integrativo e Rinnovo comparativamente maggiormente rappresentative, quali istituti contrattuali di settore.

6. *Commissione di certificazione D.Lgs. 276/2003 e D.P.R. 177/2011* - Le parti sociali firmatarie del presente Protocollo Integrativo e Rinnovo comparativamente maggiormente rappresentative comparativamente (UGL, CIU) costituenti gli Enti Bilaterali contrattuali dei ccnl previsti dal Protocollo di Accordo Interconfederale del 17 febbraio 2018, intendono offrire il servizio di certificazione dei contratti di lavoro, e la certificazione di rinunce e transazioni in sede di certificazione del contratto.

Tale servizio viene erogato attraverso la "Commissione di Certificazione Unitaria dei 9 Macro Settori", Commissione già costituita tra gli Enti Bilaterali di emanazione dei ccnl sottoscritti dalle parti sociali maggiormente rappresentative comparativamente di cui sopra (UGL, CIU aventi un membro nel CNEL) che opera in conformità e come previsto dal D.Lgs. 276/2003 e dal D.P.R. 177/2011, secondo un preciso iter dettagliatamente descritto nel suo "Regolamento". Gli associati hanno accesso a questo servizio anche attraverso il versamento dello 0,30% direttamente tramite il sistema UNIEMENS ad uno degli Enti Bilaterali che hanno sottoscritto la convenzione di costituzione della Commissione Unitaria dei 9 Macro Settori.