STUDIO DI IMPATTI 1 – FRANCIA

"Imprese e GDPR, sfide, posta in gioco e conseguenze" Prologo

Il regolamento generale sulla protezione dei dati 2016/679 del 27 aprile 2016 (GDPR), entrato in vigore il 25 maggio 2018, sostituisce il sistema dei precedenti regolamenti previsto dalla legge sulla protezione dei dati, un sistema basato sulla responsabilità degli operatori, che devono sempre dimostrare la conformità delle loro procedure al presente regolamento.

1) La specificità del regolamento: la sua applicazione immediata e attuale dal 25 maggio 2018 in tutti i paesi dell'UE senza l'esistenza di una necessità, contrariamente alle Direttive, per essere inserita nelle legislazioni nei vari Stati membri. Le procedure già in vigore in tale data devono ora rispettare le sue disposizioni.

La Commissione Nazionale per la Protezione dei Dati (Cnil) [*autorità amministrativa indipendente francese incaricata di assicurare l'applicazione della legge sulla tutela dei dati personali*], sul suo sito Web e in molte guide pratiche, analizza l'impatto dell'entrata in vigore di questo testo, in particolare per le imprese. Pertanto, questo caso di studio terrà conto del contenuto dei suggerimenti formulati dalla CNIL in merito al rapporto tra i dipendenti e la loro azienda.

Nota:

Il GDPR [*Regolamento Generale sulla Protezione dei Dati*] si applica a più settori e non prevede norme specifiche in materia per il settore del diritto del lavoro, che lascino agli Stati membri la libertà di determinare gli adeguamenti che ritengono necessari. Il disegno di legge sui dati personali, che è stato finalmente adottato dal Parlamento il 14 maggio 2018 e modifica la legge e le libertà di trattamento dei dati (legge 78-17 del 6 gennaio 1978), contiene disposizioni minime specifiche sui rapporti di lavoro, oltre al trattamento di determinati dati .

Pertanto, il nostro studio di impatto mira a presentare le modifiche introdotte dal GDPR rispetto alla legislazione precedente.

2) Il passaggio dal significato delle precedenti formulazioni (dichiarazione, autorizzazioni) contenute nella precedente direttiva 95/46 / CE del 24 ottobre 1995 a una logica di conformità in cui gli operatori sono responsabili, sotto il controllo e con il sostegno del CNIL ai sensi del nuovo regolamento europeo.

I responsabili del trattamento dei dati devono attuare tutte le misure tecniche e organizzative necessarie per garantire la protezione dei dati personali, a partire dalla progettazione del prodotto o del servizio e su base continuativa, al fine di dimostrare la conformità al trattamento dei dati in qualsiasi momento.

La conseguenza di questa responsabilizzazione delle parti interessate è l'abolizione degli obblighi di comunicazione precedentemente previsti.

In realtà, prima del suo ingresso in azienda, il Comitato economico e sociale (CESE) deve essere informato sul trattamento automatico dei dati del personale e su eventuali modifiche del trattamento (articolo L 2312-38 del Codice del Lavoro).

Questa abolizione degli obblighi di comunicazione può creare difficoltà in caso di controversia. La mancanza di una dichiarazione obbligatoria presso la Commissione Nazionale per la Protezione dei Dati (Cnil) potrebbe consentire a un dipendente che è stato penalizzato o licenziato di utilizzare prove dei fatti che si presume abbiano fatto, citando un dispositivo non segnalato. Questo non sarà più possibile.

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

3) Imprese che rientrano nel Regolamento Generale sulla Protezione dei Dati (GDPR): può riguardare qualsiasi organizzazione, indipendentemente dalle sue dimensioni, dal paese di ubicazione e dalle sue attività.

In effetti, il GDPR si applica a qualsiasi organizzazione (pubblica o privata), indipendentemente dalle sue dimensioni, paese di ubicazione o attività, in quanto elabora dati personali per suo proprio oppure no, se:
• si trova nel territorio dell'Unione Europea.
• la sua attività è direttamente rivolta agli abitanti dell'Europa.
Esempio: un'azienda con sede in Francia, che esporta tutti i suoi prodotti al di fuori dell'Unione Europea, deve conformarsi al GDPR.
Il GDPR si rivolge anche a subappaltatori che gestiscono dati personali per conto di altre organizzazioni (ad esempio, società).
I subappaltatori sono soggetti a specifici obblighi: proteggere i dati personali e la privacy dalla fase di progettazione del loro servizio o prodotto, fornire consulenza ai loro clienti, mantenere un registro delle attività di elaborazione eseguite per conto dei loro clienti. Il subappalto deve includere una clausola specifica sulla protezione dei dati personali.

4) I dati GDPR sono i cosiddetti dati personali, ovvero informazioni che consentono l'identificazione diretta (nome, cognome ad esempio) o l'identificazione indiretta (numero cliente, numero di telefono, numero di registrazione dell'auto per la gestione dei parcheggi, dati biometrici, ecc.) di una persona.
Una persona può essere identificata da un singolo dato (ad esempio AMKA) o dal confronto di un insieme di dati (persona che vive presso un indirizzo *a*, nato in questa data, abbonato alla rivista *x* e membro del sindacato *y*).
Nota:
Gli indirizzi IP e Mac sono dati personali (Cass., 1st civ 3-11-2016 n ° 15-22.595 FS-PB). La raccolta di alcuni dati richiede una particolare vigilanza, in particolare per quanto riguarda i parenti dei dipendenti, in quanto possono fornire informazioni sul loro orientamento sessuale.
Il concetto di fascicolo include qualsiasi insieme strutturato di dati personali accessibile secondo criteri definiti, indipendentemente dal fatto che il fascicolo sia conservato in un determinato punto, sia decentralizzato o distribuito funzionalmente o geograficamente (ad esempio file in ordine alfabetico o cronologico).
Il trattamento dei dati personali è un atto o una serie di atti relativi ai dati personali indipendentemente dal processo utilizzato (raccolta, registrazione, organizzazione, manutenzione, adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra modalità di offerta in forma disponibile).
Nota:
Un file contenente solo le informazioni di contatto dell'azienda (ad esempio, “Azienda A” con indirizzo postale, numero di telefono del call center e indirizzo di posta elettronica di contatto generale “companyA@email.fr”) non costituisce un trattamento di dati personali. Inoltre, il trattamento dei dati personali non è necessariamente informatizzato: anche le buste stampate sono soggette al GDPR e pertanto devono essere protette.
Il trattamento dei dati personali deve avere un obiettivo, uno scopo. La raccolta o il trattamento di dati personali non ha lo scopo di renderli utili un giorno.

5) Persone coinvolte nel GDPR

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

• Il responsabile del trattamento è la persona fisica o giuridica, o l'autorità pubblica, o l'agenzia o altra entità che, da sola o in collaborazione con altri, stabilisce le finalità e i mezzi di trattamento ed è responsabile del rispetto degli obblighi che ne derivano dal regolamento.
• La persona interessata a un trattamento è quella a cui si riferisce il trattamento.
• Il destinatario di un processo di trattamento è una persona fisica o giuridica, autorità pubblica, servizio o qualsiasi altro ente che riceve la divulgazione di dati personali, di terze parti o meno, qualsiasi persona diversa dall'interessato, il responsabile, il subappaltatore e le persone che, sotto l'autorità diretta del responsabile del trattamento o del subappaltatore, sono autorizzate al trattamento dei dati personali.

6) I principi applicati dal GDPR
Il regolamento si basa sui principi secondo cui i dati personali devono:
• aver subito un trattamento legale, equo e trasparente dell'interessato
• vengono raccolti per scopi specifici, chiari e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi;
• sono adeguati, pertinenti e limitati a quanto necessario per le finalità per le quali vengono trattati (minimizzazione dei dati)
• sono accurati e aggiornati
• vengono conservati in una forma che consenta l'identificazione delle parti interessate per un periodo non superiore a quello necessario per le finalità per le quali viene effettuato il trattamento
• vengono trattati in modo tale da garantire la corretta sicurezza dei dati personali, inclusa la protezione da trattamenti non autorizzati o illegali e da perdita, distruzione o danno accidentali (integrità e riservatezza).
Nota:
È necessario intraprendere azioni specifiche per conformarsi ai principi stabiliti nel GDPR:
• specificare i file.
• identificare processi pericolosi.
• rispettare i diritti delle persone.
• proteggere i dati.
• assicurare che, in caso di subappalto, il fornitore di servizi rispetti il GDPR
• designare un responsabile della protezione dei dati

7) Il Responsabile della protezione dei dati (RPD) è obbligatorio per le organizzazioni pubbliche e le imprese la cui attività principale è monitorare regolarmente e sistematicamente individui su larga scala o elaborare reati e reati su larga scala sensibili ai dati o correlati.
Tuttavia, anche se la società non è formalmente tenuta a designare un responsabile della protezione dei dati, la CNIL raccomanda di nominare una persona con interconnessioni interne responsabile del rispetto della normativa europea.
È responsabile del rispetto della protezione dei dati all'interno della sua organizzazione ed è principalmente responsabile di:
• informare e consigliare il responsabile del trattamento dei dati o il subappaltatore e il suo personale
• monitorare la conformità alle normative nazionali e alla legislazione sulla protezione dei dati
• consigliare la società di condurre studi di impatto sulla protezione dei dati e verificarne le prestazioni
• collaborare ed essere il punto di contatto dell'autorità di controllo.
L'RPD può essere nominato internamente dai dipendenti dell'azienda o esternamente. Può anche essere condiviso da varie organizzazioni o associazioni o federazioni professionali.
Nota:
Il concetto di elaborazione su larga scala non è definito dal GDPR e pertanto CNIL ha fornito esempi di

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

questo concetto di "elaborazione su larga scala": i processi di elaborazione che gestiscono i dati dei viaggiatori che utilizzano i mezzi pubblici o quelli gestiti dalle banche, compagnie assicurative, fornitori di servizi telefonici o ISP e si riferiscono ai dati dei loro clienti.

8) L'inventario dei dati impone l'obbligo di mantenere un registro del trattamento dei dati personali.
Sebbene questa misura si applichi solo alle aziende con almeno 250 dipendenti, la CNIL raccomanda la sua applicazione più ampia.
Lo scopo è identificare le principali attività dell'azienda che richiedono la raccolta e l'elaborazione dei dati (esempi di gestione delle risorse umane: reclutamento, gestione delle buste paga, formazione, dichiarazioni obbligatorie, tessere di iscrizione, ecc.).
Per ogni attività, dovete segnalare:
• il responsabile per l'elaborazione
• l'obiettivo perseguito
• le categorie di dati utilizzati (esempio di buste paga: cognome, nome, data di nascita, stipendio, ecc.)
• persone con accesso ai dati (destinatario - esempio: dipartimento di reclutamento, dipartimento IT, gestione, fornitori di servizi, partner)
• la durata della conservazione di questi dati (il periodo di tempo per cui i dati sono utili dal punto di vista operativo e il periodo di tempo in cui sono conservati in un file)
Il registro è sotto la responsabilità del direttore amministrattivo dell'azienda.
Secondo la CNIL, non è necessario fare riferimento a questo registro processi puramente occasionali, come file creati per un evento separato, ad esempio l'inaugurazione di un negozio.

9) Il compito affidato al responsabile del trattamento è di poter dimostrare in qualsiasi momento che i processi che gestisce sono conformi al Regolamento.
Pertanto, è importante essere in grado di determinare i dati raccolti verificando diversi punti:
• le circostanze in cui i dati sono stati raccolti: è stato ottenuto il consenso degli interessati? In caso contrario, la raccolta soddisfa specifici obblighi (raccolta richiesta per il contratto, rispetto di un obbligo legale, ad es. Trattamento dei dati sui dipendenti per la notifica alla sicurezza sociale o all'amministrazione fiscale, ecc.)?
• la natura delle informazioni fornite alle persone raccolte e trattate: sono state informate dello scopo del trattamento e dei loro diritti?
• la natura dei dati raccolti in relazione allo scopo del trattamento: solo i dati strettamente necessari al trattamento possono essere raccolti ed elaborati.
• informazioni relative al fatto che solo le persone autorizzate hanno accesso ai dati di cui hanno bisogno e che i dati non sono mantenuti oltre il necessario.

10) Casi speciali di trattamento dei dati che comportano una maggiore vigilanza
Si riferiscono a processi che hanno un oggetto o un risultato:
• Valutazione degli aspetti personali o valutazione di un individuo.
• Processo decisionale automatizzato.
• Monitoraggio sistematico delle persone: monitoraggio remoto, monitoraggio dei social network dei dipendenti, analisi delle pagine dei social network in cerca di lavoro, strumenti di gestione del tempo (scheda, ad esempio), sistemi di localizzazione geografica.
• Elaborazione di dati sensibili. Questi sono dati che rivelano la presunta origine razziale o etnica, relativa a credenze politiche, filosofiche o religiose, status sindacale, aspetto sanitario o orientamento sessuale, dati genetici o biometrici, reati o processi penali
• Elaborazione di dati su persone vulnerabili (esempio: minori).
• Usi innovativi o applicazione di nuove tecnologie (esempio: oggetto connesso).

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

• Esclusione da un diritto, servizio o contratto..
Quando l'elaborazione dei dati soddisfa almeno 2 di questi 9 criteri, deve essere eseguita una valutazione dell'impatto sulla privacy (PIA: Assessment of Impact on Privacy). CNIL ha sviluppato un software per facilitare lo svolgimento e la standardizzazione delle analisi di impatto: https://www.cnil.fr/fr/outil-pia-telechargez-et-instoulez-le-logiciel-de-la-cnil.

Nota:
L'articolo 8 della legge sulla protezione dei dati, adottato dal Parlamento il 14 maggio 2018, vieta il trattamento di dati sensibili. Tuttavia, laddove lo scopo del trattamento lo richieda, per determinate categorie di dati, questo divieto non si applicherà, in particolare per quanto riguarda il trattamento in conformità alle norme standard adottate dalla CNIL, le quali sono applicate dai datori di lavoro e riguardano dati biometrici strettamente per esigenze di controllare l'accesso ai luoghi di lavoro nonché ai dispositivi e alle applicazioni utilizzati nel contesto delle missioni assegnate a dipendenti, tirocinanti o fornitori di servizi. Per motivi di semplicità e supporto, la CNIL non richiederà una valutazione d'impatto immediata per i processi esistenti precedentemente sottoposti a CNIL prima del 25 maggio 2018 (ricevuta, dichiarazione di conformità a determinati standard, approvazione, parere del CNIL) o che sono stati iscritti nel registro delle dichiarazioni di diritto anteriore.
Le società interessate hanno un periodo di 3 anni a decorrere dal 25 maggio 2018 per realizzare questo studio di impatto. Questa tolleranza non si applica ai trattamenti precedenti al 25 maggio 2018 e che vengono regolarmente applicati ma sono stati sostanzialmente modificati dopo aver completato la precedente dichiarazione.

11) Il caso speciale del trasferimento di dati al di fuori dell'UE

In tal caso, è necessario verificare se il paese in cui i dati vengono trasmessi ha una legislazione sulla protezione dei dati e se è riconosciuto come sufficiente dalla Commissione europea. Una mappa del mondo che delinea le leggi sulla protezione dei dati è disponibile sul sito web della CNIL.
In caso contrario, la società deve salvaguardare i trasferimenti di dati al fine di garantire la protezione dei dati all'estero.

12) Informazioni dei dipedenti

Lo strumento di raccolta dei dati, indipendentemente dalla sua natura (modulo, questionario, ecc.) Dovrebbe includere le seguenti informazioni:

• l'identità e i dettagli di contatto del responsabile del trattamento e, se del caso, il rappresentante del responsabile del trattamento

• ove applicabile, i dati di contatto del responsabile della protezione dei dati

• le finalità del trattamento cui sono destinati i dati personali e la base giuridica del trattamento
• le categorie di dati personali rilevanti

• ove applicabile, i destinatari o le categorie di destinatari dei dati personali (servizio aziendale interno, fornitore di servizi, ecc.)

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

• il periodo di conservazione dei dati

• le modalità con cui le parti interessate possono esercitare i loro diritti (attraverso il loro spazio personale sul sito Web dell'azienda, attraverso un messaggio a un indirizzo e-mail dedicato, tramite posta a un servizio riconosciuto, ecc.)

• in caso di trasferimento di dati al di fuori dell'Unione Europea, il Paese interessato, l'esistenza o l'assenza di una decisione sull'adeguatezza della protezione legale dei dati ricevuti dalla Commissione Europea o il riferimento a garanzie appropriate o personalizzate e come ottenere un una copia delle garanzie o disponibile.

Inoltre, è indispensabile che queste informazioni vengano trasmesse:

• dal momento in cui i dati vengono raccolti, in quando vengono raccolti direttamente dal dipendente (durante il reclutamento, ad esempio)

• al massimo un mese dopo questa raccolta, se i dati vengono raccolti indirettamente, da un'altra fonte.

Tuttavia, queste informazioni non devono essere fornite se il dipendente le possiede già.
Nota:
In relazione al rapporto tra l'azienda e i suoi dipendenti, la CNIL raccomanda che questi ultimi siano tenuti informati ogni volta che vengono richieste informazioni (esempi: informazioni per motivi amministrativi, richiesta di formazione, modulo di colloquio, valutazione ecc.) O durante installazione di un sistema di monitoraggio in conformità con le procedure definite dall'organizzazione dell'azienda (nota di servizio, modifica del contratto di lavoro, informazioni sull'intranet, allegato sui salari, ecc.)

13) Garantire e rafforzare i diritti dei dipendenti sui propri dati: diritto di accesso, correzione, opposizione, cancellazione (diritto all'oblio), diritto alla portabilità e limitazione del trattamento.
Il GDPR richiede ai lavoratori di disporre dei mezzi per esercitare efficacemente i propri diritti attraverso un modulo di contatto su un sito Web, un numero di telefono o persino un indirizzo e-mail.
Il diritto all'oblio è il diritto di una persona di richiedere al responsabile del trattamento la cancellazione dei dati personali che lo riguardano al più presto. I motivi che giustificano l'esercizio di questo diritto sono limitati all'articolo 17 del GDPR. In generale, il GDPR richiede la cancellazione dei dati non appena non sono più utili per gli scopi per i quali sono stati raccolti. Si consiglia, oltre a specificare i tempi di cancellazione dei dati a seconda dei file, vengono introdotti meccanismi di cancellazione automatica o avvisi usati per mantenere i file. Per quanto riguarda in particolare le assunzioni, le informazioni sui candidati che non hanno avuto successo dovrebbero essere eliminate a meno che non accettino di rimanere come candidati dell'azienda (periodo di conservazione limitato a 2 anni).
Il diritto di limitare l'elaborazione significa che una persona può richiedere al responsabile del trattamento di non utilizzare determinati dati raccolti.
Il diritto alla portabilità, un'innovazione introdotta dal GDPR, è il diritto di una persona di ottenere o riutilizzare i dati relativi a lui / lei per i suoi bisogni personali, ma richiede che siano soddisfatte tre condizioni:
• i dati personali sono stati forniti dagli stessi
• i dati vengono elaborati automaticamente, con il consenso dell'interessato o per l'esecuzione di un contratto
• la portabilità non deve violare i diritti e le libertà di terzi.

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

14) La sicurezza dei dati mira alle misure da adottare, sia che si tratti della sicurezza di dati archiviati elettronicamente (file) sia che si tratti di dossier cartacei, e dipende dalla sensibilità dei dati trattati e dai rischi per le persone in caso di diffusione di dati

È necessario intraprendere varie azioni: aggiornamenti del software antivirus, modifiche regolari della password e utilizzo di password complesse e / o crittografia dei dati in alcuni casi.

L'azienda-vittima della violazione dei dati personali (i dati personali sono stati, per errore o illegalmente, danneggiati, persi, modificati, divulgati o è stato osservato un accesso ai dati non autorizzato) deve segnalare alla Cnil entro le successive 72 ore, se tale violazione è probabile che costituisca una minaccia per i diritti e le libertà degli interessati. Questa notifica viene effettuata online sul sito Cnil.

È inoltre necessario informare le persone interessate che i loro dati potrebbero essere stati compromessi.

Nota:

Se non è possibile identificare esattamente chi potrebbe essere interessato da violazioni della sicurezza, è necessario informare il pubblico, il che può costituire un fatto molto grave in termini di immagine dell'azienda.

15) Vigilanza e rafforzamento dell'entità delle sanzioni, il che significa che i responsabili del trattamento dei dati e i subappaltatori possono essere soggetti a sanzioni amministrative significative in caso di violazione delle disposizioni del regolamento: avviso, avviso formale, interruzione del trattamento, sospensione del flusso di dati, ecc.

Le ammende amministrative possono ammontare a 10 o 20 milioni di euro, a seconda della categoria del reato o, nel caso di un'impresa, dal 2% al 4% del suo fatturato mondiale annuo, a seconda di quale sia maggiore.

Quest'ultimo importo dovrebbe essere collegato al fatto che, per l'elaborazione transnazionale, le sanzioni saranno adottate congiuntamente da tutte le autorità di regolamentazione interessate, coprendo quindi eventualmente l'intera Unione europea.

In questo caso, alla società verrà imposta un'unica decisione sulle sanzioni, che sarà decisa da varie autorità di protezione.

16) Il controllo esercitato dalla CNIL per quanto riguarda la conformità al GDPR dal 25 maggio 2018 consiste nel controllare elettronicamente i locali delle agenzie attraverso un'audizione e su base documentata. Le procedure per l'avvio delle ispezioni rimangono le stesse: la decisione di condurre un'ispezione si baserà sul programma di ispezione annuale, i reclami ricevuti dalla CNIL, le informazioni che compaiono sui media o come seguito di un precedente controllo.

La principale innovazione risiede nel fatto che i controlli effettuati da organismi internazionali saranno effettuati nel contesto di una cooperazione molto ampia, che porterà a una decisione europea armonizzata.

I principi di base della protezione dei dati rimangono sostanzialmente invariati (trattamento equo, pertinenza dei dati, periodo di conservazione, sicurezza dei dati, ecc.). Di conseguenza, continueranno a essere sottoposti a scrupolosi controlli da parte della CNIL.

D'altro canto, per quanto riguarda i nuovi obblighi o i nuovi diritti derivanti dal GDPR (diritti di portabilità, analisi di impatto, ecc.), i controlli che si effettuerano riguarderanno principalmente il sostegno alle imprese, per una buona comprensione e applicazione operativa dei testi. Se gli organismi sono in buona fede, si sforzano di conformarsi e cooperare con la CNIL, tali controli normalmente non intendono condurre a procedure sanzionatorie durante i primi mesi.

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

STUDIO DI IMPATTO 2 – FRANCIA

«L'impatto del GDPR sulla divulgazione e consultazione di accordi collettivi»

Introduzione
Dal 1 ° settembre 2017, i contratti collettivi devono essere resi pubblici e pubblicati in un database nazionale, accessibile online all'indirizzo https://www.legifrance.gouv.fr/initRechAccordsEntreprise.do Lo scopo di questa banca dati nazionale è facilitare l'accesso alle disposizioni dei contratti collettivi e degli accordi e quindi rafforzare il ruolo della negoziazione commerciale.

1) Accordi soggetti a questo nuovo obbligo di pubblicazione
Gli accordi collettivi e gli accordi conclusi dal 1 ° settembre 2017 devono essere resi pubblici e pubblicati su una banca dati nazionale accessibile da Légifrance. Questo obbligo si applica indipendentemente dal livello di negoziazione: operativo, di installazione, professionale, di gruppo o settoriale.
Nota:
Viene applicato l'articolo L2231-5-1 del Codice del lavoro, il quale prevede:
"*I contratti e gli accordi a livello settoriale, di gruppo, quasi professionale, operativo e di struttura sono resi pubblici e inseriti in una banca dati nazionale, i cui contenuti sono pubblicati elettronicamente in un sistema aperto che può essere facilmente riutilizzato. Dopo la conclusione del contratto o dell'accordo , le parti possono dichiarare che parte del contratto o accordo non saranno oggetto della pubblicazione di cui al primo comma. Questo atto e il testo completo del contratto oppure l'accordo e la versione del contratto o dell'accordo destinato alla pubblicazione devono essere allegati ai documenti depositati conformemente all'articolo L. 2231-6. In assenza di un tale atto, su richiesta di una delle organizzazioni firmatarie, il contratto o l'accordo sono pubblicati in forma anonima alle condizioni previste dal Decreto del Consiglio di Stato.*
Le condizioni per l'applicazione del presente articolo sono stabilite da un decreto del Consiglio di Stato."
Eccezionalmente, dal 1 ° aprile 2018, contratti collettivi di contrattazione, contratti di risparmio dei dipendenti (partecipazione agli utili, partecipazione azionaria, piani di risparmio aziendali, lavoro autonomo e Perco), nonché accordi che definiscono il contenuto dei piani di protezione dell'occupazione non sono più soggetti a pubblicazione.
Tuttavia, questo obbligo si applica anche agli accordi di risoluzione, anche quando includono informazioni economiche e sociali sulla società.

2) Possibilità di pubblicare in versione anonima
Ai sensi degli articoli L 2231-5-1 e D 2231-7 del Codice del lavoro, la parte responsabile del deposito del contratto o del contratto è tenuta ad allegare una pubblicazione del contratto o del contratto collettivo in forma elettronica che può essere facilmente scaricato dal computer. Questa versione deve essere anonima, ovvero deve essere pubblicata senza il nome e il cognome dei negoziatori e dei firmatari. Il nome della società, il numero SIREN, il nome dei sindacati che hanno firmato, il titolo dei loro rappresentanti devono tuttavia apparire nell'accordo o nel contratto. Dopo aver ricevuto il file di archivio, Direccte trasmette il testo per la pubblicazione alla Divisione Informazioni legali e amministrative (DILA) per la pubblicazione sul sito Web Légifrance.
(www.teleaccords.travail-emploi.gouv.fr).

3) I documenti da presentare
In caso di pubblicazione completa o parziale, la persona che presenta il contratto o il contratto deve allegare i seguenti documenti alla deposizione:

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

- il testo completo e firmato dell'accordo;
- pubblicazione della versione anonima;
- una copia della lettera, e-mail o ricevuta che mostri la data di notifica del testo a tutti i sindacati rappresentativi al termine del processo di firma.
Inoltre, in alcuni casi specifici, dovrebbero essere fornite ulteriori informazioni e documenti:
- se la società ha stabilimenti separati, il testo presentato è accompagnato da un elenco di tali stabilimenti e dei loro indirizzi corrispondenti,
- quando le parti decidono che alcune parti dell'accordo non devono essere pubblicate, devono allegare l'atto di pubblicazione parziale.
- per quanto riguarda gli accordi referendari, dovrebbero essere allegati i verbali dei risultati delle consultazioni.
- documenti specifici sono richiesti anche in casi specifici (esempio: accordo salariale reale).
Questi documenti sono preferibilmente archiviati in formato PDF, ad eccezione della pubblicazione della versione anonima dell'accordo, che dovrebbe essere in formato docx (www.teleaccords.travail-emploi.gouv.fr).
Nota:
L'elenco dei documenti che devono accompagnare il deposito del contratto o del contratto collettivo è riportato nell'articolo D 2231-7 del Codice del lavoro.

4) Possibilità di pubblicazione parziale
L'articolo L 2231-5-1 del Codice del lavoro consente ai firmatari di un contratto di gruppo, di un lavoratore autonomo, di un'impresa o di uno stabilimento di decidere, dopo la conclusione dell'accordo, di non pubblicarne alcune parti.
Tuttavia, questa pubblicazione parziale deve essere formalizzata mediante atto motivato e firmato:
- da parte dei lavoratori: dalla maggioranza del numero di sindacati
- dal lato del datore di lavoro: dal rappresentante legale del gruppo, della società o dello stabilimento per i contratti conclusi a tali livelli e dai rappresentanti legali delle società interessate per i contratti di lavoro autonomo (si applica l'articolo R 2231 -1-1) del codice del lavoro).
L'atto di pubblicazione parziale, il testo da pubblicare e la sua versione integrale firmata sono allegati alla presentazione. Il contratto collettivo o accordo è pubblicato con l'indicazione che la pubblicazione è parziale.
Nota:
A partire dal 1 ° aprile 2018, i contratti professionali settoriali, professionali o simili non possono più beneficiare di questa opzione e devono essere pubblicati nella loro interezza.

5) Domande ancora in sospeso
Tuttavia, permangono domande sulla natura dell'atto di pubblicazione.
Infatti, l'atto di pubblicazione parziale, poiché non è un contratto collettivo, la sua negoziazione non è soggetta al diritto comune di contrattazione collettiva e riguarda solo i sindacati che hanno firmato l'accordo (in questo senso si può fare riferimento a RJS 11/18 783 Jeansen e Thuleau, "La pubblicità degli accordi collettivi, trasparenza e privacy").
Infine, né le leggi né i regolamenti stabiliscono le procedure per l'emissione dell'atto di pubblicazione parziale in caso di accordo con i rappresentanti dei dipendenti non rappresentati dai sindacati o avallato da 2/3 del personale su proposta del datore di lavoro . Un simile atto non sembra essere possibile per tali accordi quanto alle condizioni di firma previste nei testi.
Tuttavia, non esiste ancora una legge per affrontare questi questioni e rispondere alle domande che pongono.

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

6) Tutela degli interessi aziendali

Con una decisione unilaterale, il datore di lavoro può nascondere informazioni che danneggiano gli interessi strategici dell'azienda.

Utilizza l'opzione fornita dall'articolo L 2231-5-1 del codice del lavoro.

Questa opzione è particolarmente interessante per gli accordi le cui procedure di autorizzazione non consentono un atto di pubblicazione parziale.

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

STUDIO DI IMPATTO 3 – FRANCIA

«Con il GDPR, la protezione dei dati si applica anche ai sindacati»

Introduzione
I comitati sociali ed economici (CES) e i sindacati sono ancora in attesa della produzione di standard GDPR da parte della National Data Protection Commission (CNIL). Nel frattempo, la CNIL rimane flessibile sulla conformità.
Prima dell'attuazione del Regolamento generale europeo sulla protezione dei dati (GDPR) in Francia, il Comitato economico e sociale (ESC) di una società o di uno stabilimento poteva essere esonerato dalla divulgazione di dati personali alla CNIL. Ma dal 25 maggio 2018, con l'entrata in vigore del GDPR, queste disposizioni della CNIL non hanno più valore legale. Oggi, la protezione dei dati soggetta al GDPR include anche i CES. Infatti, nel contesto della sua missione e responsabilità (in particolare per quanto riguarda le attività sociali e culturali), il Comitato è obbligato a raccogliere ed elaborare dati personali, in particolare i dati dei dipendenti sulla loro vita familiare e personale e la loro salute: cognome, nome, indirizzo, stato civile, luogo, telefono ed indirizzo e-mail, stato di salute, attività sociali e culturali ecc. Inoltre, in alcuni casi, vengono trasmesse alcune informazioni personali dei dipendenti nel contesto della consultazione obbligatoria (remunerazione ecc.).

Pertanto, il CES deve conformarsi al GDPR nel trattamento di questi dati:
- Ottenere il consenso dei dipendenti al trattamento dei propri dati personali.
- Informare i dipendenti dei loro diritti.
- attuare adeguate misure tecniche e organizzative per garantire ed essere in grado di dimostrare che il trattamento è conforme al GDPR.
- Tenere un registro di elaborazione.
- Progettare misure per garantire la riservatezza dei dati trattati.
- Nomina di un rappresentante dell'ESC per la protezione dei dati personali.

Il Comitato dovrebbe pertanto stabilire norme precise per tutti i dati personali raccolti e renderli accessibili al pubblico ai dipendenti. L'ESC deve quindi proteggere tutti i dati in suo possesso. Deve rassicurare i dipendenti che non sarà accessibile a persone non autorizzate. Il Comitato si impegna inoltre a non abusare di questi dati. In altre parole, li tiene per uno scopo. Il Comitato non ha il diritto di utilizzare questi dati per altri scopi. Deve avere l'approvazione preventiva della persona o delle persone interessate.

Compilazione graduale dei registri delle attività di elaborazione
L'articolo 30 del GDPR prevede l'istituzione di un registro delle attività di trattamento. Questo registro consente di identificare l'elaborazione dei dati e di rivedere ciò che l'ESC fa con i dati personali. È un documento in cui verranno registrati tutti i dati personali. La CNIL offre, ad esempio, un modello di registro (allegato 1). Il modello per questo documento è gratuito. Può essere progettato digitalmente o presentato in forma stampata o scritta a mano. Questo registro è uno strumento per monitorare e dimostrare la conformità CSE al GDPR.
Il registro delle attività di trattamento dei dati consente l'identificazione del trattamento dei dati e la presentazione dei dati personali.
3 passaggi per sviluppare il registro delle attività di modifica:
- nomina di un responsabile della protezione dei dati;
- individuazione e modifica di set di dati per attività;
- Compilazione di un foglio per ogni attività che dettaglia il trattamento dei dati.

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).

Il ruolo del Responsabile della protezione dei dati (DPO)

L'ESC può nominare un responsabile della protezione dei dati (DPO) per aggiornare il registro delle attività di trattamento dei dati personali e garantire la conformità con il GDPR. Questa misura non è obbligatoria ma è altamente raccomandata per le aziende che gestiscono molti dati personali. La designazione di un RPD può rivelarsi utile alla luce delle informazioni e dei consigli forniti dall'ESC al controllore o al subappaltatore.

Nessun tempo aggiuntivo è attualmente assegnato al responsabile della protezione dei dati. C'è il timore che questo nuovo sistema porti a ulteriori responsabilità e carichi di lavoro per i rappresentanti eletti, in particolare il rappresentante designato. È probabile che questo progetto richieda tempo, soprattutto nei prossimi mesi, per molti funzionari eletti, mentre la conformità ESC è in corso.

Il consenso del dipendente

Il GDPR presuppone che venga richiesto il consenso dei dipendenti per procedere alla raccolta dei dati. I rappresentanti dei dipendenti devono determinare come ottenere questo consenso, se si tratta di un documento scritto e firmato dal dipendente o di un controllo sul sito Web. In ogni caso, i mezzi utilizzati devono indicare chiaramente l'oggetto all'interessato che accetta il trattamento dei propri dati.

Pertanto, l'ESC può chiedere ai dipendenti:

- accesso alle informazioni che li riguardano
- correzione dei loro dati personali
- eliminazione del loro profilo se necessario.

Per questo motivo, il Comitato dovrebbe spiegare chiaramente ai dipendenti la procedura o le procedure da seguire. Ciò garantirà un migliore rispetto del regolamento.

Il Comitato è obbligato ad adottare il regolamento interno che stabilisce i suoi metodi di funzionamento, le sue regole e quelle relative ai suoi rapporti con i dipendenti nell'esercizio delle sue funzioni. Al fine di conformarsi, un gran numero di consigli di lavoro / ESC ha incorporato una specifica clausola sulla privacy nei loro regolamenti interni.

Questo progetto è finanziato con il sostegno della Commissione europea. Programma RAFFORZAMENTO DELLA PARTECIPAZIONE (DG Employment- VS / 2019/0057).