DAYCO EUROPE S.R.L.

PROCEDURA

Policy sull'utilizzo delle attrezzature informatiche. Della posta elettronica aziendale, Intranet, VoIP e telefonia mobile

Gennaio 2022

Sommario

PREMESSA

L'utilizzo delle risorse informatiche e telematiche da parte di ciascun dipendente di Dayco Europe S.r.l. (di seguito "**Dayco**" o la "**Società**") deve sempre ispirarsi al principio di diligenza e correttezza, comportamenti questi che sono alla base di un corretto rapporto di lavoro.

La progressiva e capillare diffusione delle tecnologie informatiche e in particolare dell'accesso alla rete Internet, infatti, può esporre Dayco a numerosi rischi, sia di carattere strettamente patrimoniale che penale, creando problemi alla sicurezza interna delle informazioni sensibili per il *core business* aziendale e alla sua immagine pubblica.

.1 FINALITÀ E AMBITO DI APPLICAZIONE

Lo scopo del presente documento (di seguito "**Policy**") è quello di fornire un quadro d'insieme sulle più idonee misure di sicurezza richieste da Dayco per il corretto utilizzo da parte di ciascun dipendente degli strumenti informatici, della posta elettronica aziendale e della navigazione sulla rete Internet.

Dayco, inoltre, in qualità di Titolare del trattamento dei dati personali (di seguito "**Titolare**"), ritiene opportuno dotarsi di questa Policy allo scopo di adempiere agli obblighi fissati dal Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "**Regolamento**") e dalle "*Linee guida del Garante per posta elettronica e internet – 10 marzo 2007*" (di seguito "**Provvedimento**") emanate dal Garante per la protezione dei dati personali (di seguito "**Garante Privacy**"), nonché per rispettare gli *standard* internazionali in materia di sicurezza informatica e delle informazioni.

La presente Policy è stata predisposta a uso esclusivamente interno di Dayco e, pertanto, non potrà essere riprodotta, divulgata, copiata, utilizzata e/o altrimenti resa pubblica o essere diffusa a terzi in assenza di una previa approvazione scritta, né potrà costituire base informativa e/o valutativa per finalità diverse da quelle per le quali è stata predisposta.

La presente Policy, che si basa esclusivamente sulle norme del diritto italiano e sulla normativa europea richiamata, si applica a tutte le sedi e a tutti gli amministratori, i dirigenti, i dipendenti, i collaboratori e/o soggetti terzi che utilizzino attrezzature informatiche di Dayco o che accedano per qualsivoglia ragione ai suoi sistemi informatici.

.2 REGOLE GENERALI E DESTINATARI

La presente Policy abroga e sostituisce tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate.

Copia della presente Policy sarà messa a disposizione:

- dei dipendenti, tramite e-mail di notifica della pubblicazione della presente Policy sulla Intranet aziendale e affissione in bacheca;
- dei distaccati, dei somministrati e del personale in *stage* attraverso la consegna al momento dell'inserimento in azienda da parte dell'Ufficio Risorse Umane.

È dovere di ogni dipendente applicare il complesso di regole stabilite da questa Policy e dalle normative qui referenziate, al fine di contribuire personalmente alla tutela del patrimonio delle informazioni aziendali e alla sicurezza dei suoi sistemi informatici.

La mancata applicazione delle norme contenute in questa Policy costituisce un'inadempienza contrattuale e, pertanto, potrà essere perseguita nei modi e nei termini stabiliti dai contratti e dalle opportune leggi di settore.

Il rispetto della presente Policy e delle altre disposizioni in materia di sistemi o apparati elettronici non esonera ciascun destinatario anche dal rispetto di tutte le altre disposizioni, provvedimenti, circolari, regolamenti, ecc., emanati da Dayco per regolare gli ulteriori aspetti dell'attività lavorativa (come, ad esempio, le regole in materia di salute e sicurezza sui luoghi di lavoro, quelle sulla *security*, ecc.).

Qualunque soggetto, anche non dipendente, a qualsiasi titolo abilitato all'utilizzo dei sistemi e/o degli strumenti informatici di Dayco è tenuto alla massima riservatezza in merito alle loro caratteristiche, al loro metodo di funzionamento, ovvero alle misure di sicurezza adottate per la loro protezione.

La presente Policy, come anticipato, è stata predisposta ad uso esclusivamente interno.

Questo comporta che la divulgazione all'esterno, la perdita, la manomissione o l'uso indebito delle informazioni presenti in questa Policy comportano un rischio per Dayco. Pertanto, i destinatari di questa Policy sono tenuti a trattare le presenti informazioni per le sole finalità e con le modalità connesse alle loro responsabilità e mansioni lavorative, nonché a non diffondere o comunicare in alcun caso le stesse oltre la cerchia dei soggetti sotto riportati.

I destinatari delle informazioni contenute in questa Policy sono:

- tutti gli amministratori, i dirigenti, i dipendenti di Dayco e tutti coloro che, in virtù di un rapporto di lavoro o fornitura (per esempio, lavoratori somministrati e/o in distacco, consulenti, collaboratori, fornitori, *business partner*, ecc.) utilizzino – anche temporaneamente – i sistemi informativi e/o le apparecchiature elettroniche di proprietà di Dayco.

.3 GLOSSARIO

"Autenticazione informatica": l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"Amministratore di sistema": la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ivi compresi gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;

"Archivio": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

"Credenziali di autenticazione": i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

"Dati identificativi": i dati personali che permettono l'identificazione diretta dell'interessato;

"Dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

"Dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

"Soggetti autorizzati al trattamento": le persone fisiche che sono autorizzate e adeguatamente istruite per svolgere il trattamento dei dati personali sotto l'autorità del titolare del trattamento o del responsabile del trattamento;

"Interessato": la persona fisica cui si riferiscono i dati personali;

"Pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

"Responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

“Strumenti informatici”: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico, informatico o comunque automatizzato con cui si effettua il trattamento dei dati personali;

“Titolare del trattamento”: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

“Trattamento”: qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione;

“Violazione di dati personali”: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.

.4 NORMATIVA DI RIFERIMENTO.

[1] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (“*Regolamento Generale sulla Protezione dei Dati*”);

[2] Garante per la protezione dei dati personali – “*Lavoro: le linee guida del Garante per posta elettronica e Internet – 10 marzo 2007*”;

[3] Garante per la protezione dei dati personali – “*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008*”.

[4] L. 20 maggio 1970, n. 300, denominata “*Statuto dei lavoratori*”.

[5] D.lgs. 14 settembre 2015, n. 151, recante “*Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183*”.

.5 OBBLIGHI DELLA SOCIETÀ

In ottemperanza del principio di responsabilizzazione, a cui il Titolare si ispira, i trattamenti effettuati da Dayco rispettano le garanzie poste in essere dal legislatore italiano ed europeo in materia di protezione dei dati e si svolgono nell'osservanza dei seguenti principi:

a. **principio di liceità, correttezza e trasparenza**, secondo il quale i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dei lavoratori, in modo da scongiurare l'eventuale svolgimento di trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa ed effettuati all'insaputa o senza la piena consapevolezza dei lavoratori;

b. **principio di limitazione della finalità**, secondo cui i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che non sia incompatibile con tali finalità;

c. **principio di minimizzazione dei dati**, secondo cui i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d. **principio di esattezza**, secondo il quale i dati personali sono esatti e, se necessario, aggiornati;

e. **principio della conservazione**, secondo cui i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f. **principio di integrità e riservatezza**, secondo cui i dati personali sono trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

In quest'ottica, Dayco tratta i dati dei lavoratori nella misura meno invasiva possibile, demandando le attività di monitoraggio ai fini di sicurezza dei dati e degli strumenti informatici esclusivamente a quei soggetti opportunamente preposti e designati, nonché effettuando eventuali controlli esclusivamente in maniera mirata sull'area di rischio, tenuta in debito conto la normativa sulla protezione dei dati e, se pertinente, il principio di segretezza della corrispondenza e lo Statuto dei lavoratori.

In base ai principi finora richiamati, attraverso la presente Policy, Dayco indica quali siano le modalità di utilizzo degli strumenti di lavoro messi a disposizione considerate più corrette e se, in che misura e con quali modalità, vengano effettuati i controlli.

La presente Policy ha l'intento di adempiere quest'obbligo.

Inoltre, Dayco ha predisposto tutte le accortezze necessarie affinché i dati personali contenuti nelle postazioni di lavoro informatiche siano protetti contro il rischio d'intrusione – tanto dall'esterno (Internet) che dall'interno (rete locale) – e dall'azione di programmi di cui all'art. 615-*quinquies* del codice penale, attraverso l'utilizzazione di idonei strumenti elettronici, mantenuti costantemente aggiornati. Anche i programmi della postazione di lavoro sono mantenuti costantemente aggiornati, come per legge, al fine di prevenire le vulnerabilità degli strumenti elettronici e a correggerne i difetti (i cosiddetti "*bug*").

Sono state predisposte, altresì, le opportune istruzioni organizzative e tecniche volte a prevedere il salvataggio dei dati presenti nelle aree utenti e nelle aree comuni della rete aziendale, così come dei dati della posta elettronica. Sono state previste e adottate, inoltre, le opportune procedure volte a garantire il ripristino dell'accesso alle informazioni o agli strumenti elettronici danneggiati in un arco di tempo non superiore ai 7 (sette) giorni lavorativi.

Infine, è stata predisposta da Dayco una specifica "*Procedura operativa per la dismissione delle apparecchiature elettriche ed elettroniche*", volta a proteggere le informazioni aziendali e i dati personali anche nella fase di dismissione di dette apparecchiature. Resta inteso che, nel caso in cui fosse necessario dismettere tali attrezzature, si dovrà fare riferimento al proprio responsabile che contatterà il soggetto aziendale competente. Resta altresì fermo peraltro che, qualora si preveda il riutilizzo di detti supporti da parte di altri lavoratori non autorizzati al trattamento dei medesimi dati, le informazioni in essi precedentemente contenute saranno rese non intelligibili e tecnicamente non ricostruibili.

.6 OBBLIGHI DEI LAVORATORI

Di seguito vengono specificati gli obblighi e le norme di condotta obbligatorie per ciascun lavoratore e per tutti coloro che, in virtù di un rapporto di lavoro o fornitura, trattano informazioni ovvero utilizzano sistemi informativi o apparecchiature elettroniche di proprietà di Dayco.

.6.1 UTILIZZO DEL PERSONAL COMPUTER

Il *personal computer* (PC) dato in dotazione a ciascun lavoratore è da intendersi esclusivamente come uno strumento di lavoro.

Ogni suo utilizzo improprio può contribuire a creare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza delle informazioni sensibili per il *core business* aziendale e all'immagine pubblica di Dayco.

Ogni dipendente, pertanto, è responsabile dell'utilizzo e della custodia degli strumenti informatici ricevuti in dotazione. Alla luce di ciò, salvo autorizzazione della Direzione del Personale e con l'intervento degli Addetti dei Sistemi Informativi di Dayco, a ciascun lavoratore è fatto esplicito divieto di:

- modificare qualsiasi caratteristica *hardware* e *software* impostata sul proprio *personal computer*;
- installare e/o eseguire qualsiasi tipologia di programmi informatici diversi da quelli preinstallati da Dayco, anche nel caso in cui si tratti di *software* opportunamente licenziato, di *software* in prova ("*shareware*"), ovvero di *software* gratuito e liberamente scaricabile da Internet ("*freeware*");
- scaricare da Internet o da altri supporti, copiare e/o archiviare – anche temporaneamente – sul *personal computer* in dotazione qualsiasi genere d'informazioni che violino il diritto d'autore e/o che possano contenere minacce informatiche (come, a mero titolo esemplificativo e non esaustivo, *file* audio, video, eseguibili, ecc.);
- cedere a soggetti non autorizzati il proprio *personal computer*, soprattutto successivamente al superamento della fase di autenticazione;
- lasciare incustodito e accessibile il proprio *personal computer* senza aver precedentemente provveduto a bloccare l'accesso alla postazione attraverso l'apposito comando (CTRL+ALT+CANC e successivamente cliccare su "Blocca il computer"), al fine di evitarne un utilizzo improprio in caso di assenza anche temporanea. In ogni caso, dopo un periodo congruo di inutilizzo della postazione di lavoro, l'accesso verrà bloccato in automatico;
- archiviare i *files* inerenti le attività lavorative, ivi compresi gli archivi destrutturati (ad es., *file Excel*, *database Access*, ecc.), soprattutto se contenenti dati personali e/o particolari, sui dischi locali del *personal computer* assegnato. Tali *file* dovranno esser conservati e salvati in aree condivise in rete, che avranno una capacità massima di conservazione dei dati definita. Resta inteso, infatti, che i dischi locali non saranno oggetto di alcuna procedura di *backup*. Quindi, in caso di guasti, smarrimento o furto i dati non potranno in alcun modo essere recuperati. Tuttavia, solo per chi utilizza *personal computer* portatili, Dayco mette a disposizione un'area sui dischi locali per memorizzare i dati aziendali. Quest'area sarà sincronizzata con le unità di rete e come tale sottoposta a *backup*.

- eliminare o comunque rendere inaccessibile qualsiasi tipologia di informazione lavorativa dal proprio *personal computer* in caso di cessazione del rapporto di lavoro.

Al fine di proteggere i *file* rendendoli inaccessibili (o difficilmente accessibili) a soggetti terzi, si consiglia, inoltre, di utilizzare le funzioni di "crittografia con *password*" disponibili nei *software* che compongono il pacchetto *Microsoft Office* dato in dotazione a ciascun utente. Ciò, soprattutto al fine di evitare, in caso di smarrimento, furto o accesso non autorizzato a fronte di attacchi informatici, che informazioni personali, particolari e/o riservate dell'azienda siano accessibili a soggetti terzi.

Le postazioni di lavoro, inoltre, devono essere spente al termine della giornata lavorativa, salvo espliciti e contrari avvisi da parte degli addetti ai sistemi informativi.

Essendo uno strumento di lavoro, ogni utente è avvisato che le informazioni presenti all'interno del *personal computer* (PC) assegnato devono essere considerate e trattate come lavorative e non personali. Nonostante ciò, purché non vengano violate le regole previste all'interno della presente Policy, qualora il dipendente abbia necessità di salvare e conservare una limitata quantità di dati e informazioni personali non inerenti l'attività lavorativa, deve provvedere a creare sul proprio *desktop* una cartella denominata "Personale" in cui inserire i suddetti dati. Detta cartella non sarà comunque sottoposta ad attività di *backup* da parte di Dayco. La quantità di dati conservati in questa cartella non può comunque mai superare i 300 MB.

In caso di cessazione per qualsivoglia ragione del rapporto di lavoro, il dipendente, prima di lasciare il posto di lavoro, deve provvedere alla rimozione della cartella "Personale" dal proprio *personal computer* aziendale, sia fisso che portatile. In mancanza, Dayco provvederà ad effettuare questa operazione alla prima occasione utile.

In conformità con i principi di necessità, pertinenza e non eccedenza del Regolamento Europeo, Dayco si riserva fin da ora il diritto di poter eventualmente accedere in qualunque momento, anche successivamente alla cessazione del rapporto di lavoro, alle informazioni e ai dati presenti al suo interno per finalità lavorative, di continuità operativa dell'azienda e/o di salvaguardia dei propri diritti in sede giudiziaria.

L'utente è responsabile, altresì, del *personal computer* portatile eventualmente assegnatogli da Dayco e deve custodirlo con diligenza, sia durante gli spostamenti che nel corso del normale utilizzo. Ai *personal computer* portatili si applicano tutte le regole di utilizzo e i divieti previsti all'interno di questa Policy per i *personal computer* fissi. In particolare, si ricorda che, a maggior ragione durante il loro utilizzo all'esterno delle nostre strutture, il *computer* portatile non deve mai essere lasciato incustodito e deve essere adeguatamente preservato nei luoghi e con i mezzi più idonei per la sua ottimale protezione.

È fatto obbligo che ciascun dispositivo venga custodito con estrema diligenza. In caso di furto o smarrimento, l'utente assegnatario del *personal computer* ha l'obbligo d'informare tempestivamente il proprio diretto responsabile di funzione e gli addetti ai sistemi informativi di Dayco, nonché di denunciare tempestivamente l'accaduto alle Forze dell'Ordine, fornendo a Dayco, entro 24 ore dall'evento, la copia dell'atto di denuncia. Atto di denuncia che deve necessariamente contenere anche la marca e il modello.

È fatto obbligo che ciascun dispositivo venga custodito con estrema diligenza. In caso di furto o smarrimento, l'utente assegnatario del dispositivo ha l'obbligo di seguire le indicazioni dell'apposita procedura disponibile sulla Intranet aziendale.

Dayco, infine, si riserva in qualunque momento il diritto di procedere, anche senza preavviso, alla rimozione di ogni *file* o applicazione si dovesse ritenere pericolosa per la sicurezza del patrimonio informativo aziendale, che violi le regole previste all'interno di questa Policy o che, ad ogni modo, alteri la configurazione originaria della postazione di lavoro dell'utente.

Inoltre, si precisa fin da ora che, al fine di fornire la necessaria assistenza tecnica agli utenti, il personale incaricato del supporto alle postazioni di lavoro si riserva fin da ora la facoltà di accedere alle suddette sia *in loco*, che da remoto.

.7 CONTINUITÀ DELL'ATTIVITÀ LAVORATIVA IN CASO DI ASSENZA DEL LAVORATORE

Solo il lavoratore che è dotato di una postazione di lavoro informatica personale può accedere ad essa utilizzando le proprie credenziali di autenticazione.

Un'eccezione a questa regola ricorre solo nel caso in cui si verifichino contemporaneamente tutte e tre le seguenti condizioni:

- prolungata assenza o impedimento del lavoratore;
- l'accesso ai dati e agli strumenti elettronici del lavoratore assente risulti essere indispensabile e indifferibile;
- l'accesso ai dati e agli strumenti elettronici del lavoratore assente sia caratterizzato da concrete necessità di operatività e di sicurezza del sistema.

Solo al verificarsi delle tre condizioni sopra esposte, il responsabile di funzione – mediante un'e-mail inviata all'indirizzo privacy@pec.daycoeurope.com – potrà richiedere per iscritto al Titolare del trattamento di resettare la *password* del dipendente motivando la richiesta. Acquisita la richiesta, il Titolare del trattamento darà istruzioni via e-mail all'Amministratore di sistema di resettare la parola chiave (*password*) di autenticazione della postazione di lavoro elettronica del lavoratore e accedere ai dati e agli strumenti elettronici.

Di tale attività verrà redatto a cura del Titolare del trattamento un apposito verbale e il lavoratore interessato verrà prontamente informato dell'accaduto alla prima occasione utile.

.8 GESTIONE DELLE PASSWORD

L'accesso ad ogni postazione di lavoro informatica è governato da un sistema d'identificazione personale basato sull'utilizzo di credenziali di accesso (consistenti in una o più accoppiate di *username* e *password*), che ne permettono l'utilizzo nei modi e nelle forme definite da ciascun profilo aziendale esclusivamente al lavoratore o a gruppi di lavoratori autorizzati.

Le credenziali di accesso sono e devono essere conosciute esclusivamente dal soggetto o dal gruppo di soggetti per i quali sono state predisposte. È altresì lecito che dette credenziali possano essere contenute in un dispositivo di autenticazione in possesso e uso esclusivo del lavoratore, eventualmente associato anche a un codice identificativo o a una parola chiave, dei quali il soggetto è da considerarsi sempre responsabile sia sotto il profilo della segretezza (*username*/*password*), che sotto quello della custodia (dispositivo di autenticazione).

La parola chiave (*password*) deve essere composta da almeno 8 (otto) caratteri alfanumerici (lettere minuscole, maiuscole e numeri), meglio se con l'aggiunta anche di caratteri "speciali".

Non deve contenere, inoltre, riferimenti direttamente riconducibili al lavoratore e deve essere obbligatoriamente rimpiazzata al suo primo utilizzo e, successivamente, almeno ogni 3 (tre) mesi.

L'utente è tenuto a conservare nella massima segretezza la parola di accesso e/o qualsiasi altra informazione legata al processo di autenticazione/autorizzazione e a modificare immediatamente la *password* nel caso in cui sia a conoscenza che la stessa abbia perso il suo carattere di segretezza. Qualora l'utente sospetti che la *password* abbia perso il suo carattere di segretezza e che possano in conseguenza di ciò essere state commesse violazioni informatiche il medesimo dovrà darne immediata comunicazione all'Amministratore di sistema.

Il codice di autenticazione è univoco e non sarà assegnato – nemmeno in tempi diversi – a soggetti differenti, il cui *account*, anzi, sarà prontamente disattivato qualora non venga utilizzato perlomeno nell'arco di 6 (sei) mesi. Unica eccezione a questa regola è prevista nel caso in cui l'*account* sia stato creato per soli scopi di gestione tecnica e il prolungamento della sua durata oltre il termine legale stabilito dal Regolamento Europeo sia stato preventivamente autorizzato.

Le credenziali di autenticazione saranno comunque prontamente disattivate in caso di perdita della qualità che consente al lavoratore l'accesso ai dati aziendali e/o personali.

Al fine di agevolare sul piano organizzativo l'accesso alle informazioni contenute nelle aree condivise, il Titolare del trattamento ha previsto uno specifico sistema di autorizzazione. Periodicamente, e comunque almeno annualmente, sarà compito del Titolare del trattamento attraverso l'Amministratore di sistema verificare la sussistenza delle condizioni per la conservazione dei suddetti profili di autorizzazione.

Di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la *password* assegnata è responsabile l'utente o il gruppo di utenti assegnatari del codice, che ne rispondono nei confronti di Dayco ed eventualmente dei terzi.

.9 UTILIZZO DELLA RETE TELEMATICA INTERNA AZIENDALE

La rete telematica aziendale è l'insieme delle tecnologie – apparati e programmi – mediante le quali si realizza la connettività interna tra i vari componenti del sistema informatico aziendale. La perfetta e continuativa disponibilità della stessa è quindi fattore strategico per il funzionamento operativo di Dayco.

L'accesso alla rete può avvenire direttamente, ovvero attraverso connessioni fisiche presenti nelle sedi dell'azienda, oppure da remoto, mediante software di collegamento VPN che consente l'accesso sicuro alla rete interna aziendale.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi da quelli per cui sono state predisposte. Pertanto, qualunque *file* che non sia legato all'attività lavorativa non può essere dislocato – nemmeno temporaneamente – in dette unità di rete.

Su dette unità, inoltre, vengono regolarmente svolte attività di controllo, amministrazione e *backup* da parte dell'Amministratore di sistema.

Dayco effettua giornalmente il *backup* dei dati in modo automatico, prevedendo per gli utenti esclusivamente la copia di sicurezza delle cartelle presenti all'interno dell'area utente, delle aree comuni/condivise e/o della Intranet aziendale. Ciascun *file* di lavoro salvato all'esterno delle suddette aree non verrà salvato e, in caso di malfunzionamenti, potrebbe essere irrimediabilmente perso. Perciò, è fatto specifico obbligo a ciascun dipendente di salvare i *file* inerenti le attività di lavoro esclusivamente nelle cartelle presenti all'interno dell'area utente, delle aree comuni/condivise e/o della Intranet aziendale. I *backup* dei suddetti dati saranno conservati da Dayco per un massimo di 6 (sei) mesi.

Le *password* d'ingresso alla rete e ai programmi di rete sono segrete e vanno comunicate e gestite secondo le procedure in precedenza impartite. È fatto assoluto divieto di entrare nella rete interna e nei programmi utilizzando credenziali di autenticazione di qualsiasi altro utente, tranne per i casi di utenze di lavoro condivise.

L'Amministratore di sistema, anche senza preavviso, può in qualunque momento procedere alla rimozione di ogni *file* o applicazione che dovesse ritenere pericolosa per la sicurezza, sia sui PC dei lavoratori che sulle unità di rete.

Inoltre, è cura del lavoratore effettuare la stampa di documenti contenenti dati personali solo se strettamente necessaria alle esigenze di lavoro e di ritirarla prontamente dai vassoi delle stampanti di rete messe in comune. Nel caso si debbano stampare informazioni riservate, è fatto obbligo di presidiare personalmente l'area ove avviene la stampa, soprattutto qualora il dispositivo non offra funzionalità di stampa protette mediante *password* o *badge* aziendale. Per quanto attiene la cura degli strumenti di stampa, il lavoratore è tenuto a segnalare prontamente qualsiasi malfunzionamento direttamente al Centro Unico di Supporto. È buona regola, comunque, se ed ove possibile, evitare di stampare su stampanti comuni documenti o *file* riservati.

Alla luce di quanto finora evidenziato, è fatto esplicito divieto di:

- utilizzare la rete interna aziendale per fini non espressamente previsti e/o autorizzati e per scopi che non siano strettamente lavorativi;
- connettere in rete locale apparecchiature elettroniche (PC, stampanti, ecc.) o qualsiasi altro genere di apparato (*router*, *switch*, ecc.) che possa alterare la configurazione della rete interna e/o danneggiare le applicazioni.

Dayco si riserva fin da ora il diritto di rimuovere, in qualunque momento e anche senza alcun preavviso, qualsiasi tipologia di apparecchiatura elettronica o di *software* installato sulla rete interna aziendale e che non sia stato in precedenza autorizzato.

.10 UTILIZZO DEL SISTEMA DI TELEFONIA TRADIZIONALE E/O ATTRAVERSO LO STANDARD H323

Per gestire le conversazioni telefoniche sia all'interno dell'azienda, che verso la rete telefonica tradizionale e cellulare, Dayco utilizza un sistema di telefonia basato sullo standard H323.

Salvo casi eccezionali, l'utilizzo del sistema è autorizzato esclusivamente per soli scopi lavorativi e l'abuso potrà essere sanzionato. Potranno, inoltre, essere effettuati controlli sulla rendicontazione fornita dai gestori di rete a Dayco.

Dayco si riserva il diritto di utilizzare sistemi elettronici volti a verificare il livello di spesa delle utenze telefoniche assegnate e l'analisi delle direttrici di chiamata, fatto salvo quanto previsto dall'art. 4 della Legge n. 300/1970 (Statuto dei lavoratori) e successive modificazioni.

Salvo i casi in cui la conservazione dei dati sia oggetto di contestazione e Dayco sia chiamata a tutelare i propri diritti in sede giudiziaria, a norma dei principi suelencati e, in particolare, del principio di conservazione del Regolamento, le informazioni relative ai livelli di spesa delle singole utenze telefoniche assegnate e delle direttrici di chiamata saranno conservati per un periodo non superiore ai 6 (sei) mesi.

.11 USO DELLA POSTA ELETTRONICA AZIENDALE (EMAIL E PEC)

La casella di posta elettronica tradizionale e/o di posta elettronica certificata (PEC) assegnata da Dayco a ciascun lavoratore o a gruppi di utenti ben definiti è esclusivamente uno strumento di lavoro. Coloro i quali sono assegnatari di una o più caselle di posta elettronica (tradizionale e/o PEC), pertanto, sono responsabili del loro corretto utilizzo.

Essendo uno strumento di lavoro, ogni utente è avvisato che le informazioni presenti all'interno della casella di posta elettronica aziendale assegnata (tradizionale e/o PEC) devono essere considerate e trattate come corrispondenza e documentazione lavorativa e non personale. Nonostante ciò, in deroga a quanto previsto nel presente paragrafo e purché non vengano violate le regole previste all'interno della presente Policy, qualora il dipendente abbia necessità di utilizzare la casella di posta elettronica aziendale per comunicazioni private e personali non inerenti l'attività lavorativa, deve provvedere a cancellarli immediatamente dalla cartella "Posta in arrivo" e "Posta inviata", come pure dal "Cestino".

In conformità con i principi di necessità, pertinenza e non eccedenza del Regolamento Europeo, Dayco si riserva fin da ora il diritto di poter eventualmente accedere in qualunque momento alle informazioni e ai dati presenti al loro interno per finalità lavorative, di continuità operativa dell'azienda e/o di salvaguardia dei propri diritti in sede giudiziaria.

Si precisa, inoltre, che la casella di posta elettronica certificata (PEC) ha valore legale. Pertanto, ogni utilizzo improprio da parte di qualsivoglia utente verrà valutato alla luce delle specifiche normative vigenti.

Dayco effettua il *backup* dei dati presenti all'interno di ciascuna casella di posta elettronica aziendale giornalmente in modo automatico e conserva questi dati per 7 (sette) giorni.

Dayco, pur proteggendo con le più adeguate misure di sicurezza i sistemi di gestione delle caselle *e-mail* da messaggi potenzialmente pericolosi, fa comunque esplicito divieto a tutti gli utenti di:

- utilizzare l'indirizzo di posta elettronica aziendale per l'iscrizione e la partecipazione a dibattiti, *forum* o *mailing-list*, ecc., salvo comprovate esigenze lavorative;
- utilizzare l'indirizzo di posta elettronica aziendale per attività improprie o eticamente riprovevoli;
- aprire *e-mail* e/o soprattutto gli allegati in particolar modo se provenienti da mittenti sconosciuti/inconsueti o che abbiano anche solo un contenuto insolito; in caso di dubbio è fatto obbligo di avvisare preventivamente gli addetti ai sistemi informativi di Dayco, che daranno istruzioni in merito;
- inviare o dar corso a catene telematiche di messaggi (anche dette "*Catene di Sant'Antonio*").

Dayco, inoltre, fa obbligo a tutti gli utenti di:

1. utilizzare le apposite funzionalità di sistema che, in caso di assenza (ad es., per ferie o attività di lavoro fuori sede), consentono di inviare automaticamente messaggi di risposta contenenti le "coordinate" (elettroniche e/o telefoniche) di un altro lavoratore, ovvero delle altre eventuali modalità utili a contattare Dayco. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura sopra descritta, Dayco si riserva il diritto di disporre lecitamente l'attivazione di un analogo accorgimento attraverso l'Amministratore di Sistema, dandone comunicazione al dipendente.

2. mantenere in ordine la casella di posta elettronica, cancellando documenti superflui e, soprattutto, allegati ingombranti non più utili ai fini lavorativi.

Dayco, infine, si riserva in qualunque momento il diritto di procedere alla rimozione di ogni *file* si dovesse ritenere pericoloso per la sicurezza del patrimonio informativo aziendale o che, ad ogni modo, alteri la configurazione originaria della posta elettronica dell'utente.

.12 USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

La rete Internet è ormai divenuta uno strumento operativo di comunicazione imprescindibile e il *personal computer* abilitato alla navigazione costituisce a tutti gli effetti uno strumento aziendale necessario allo svolgimento dell'attività lavorativa.

Tuttavia, un suo utilizzo indiscriminato può rendere Dayco vulnerabile sotto il profilo della sicurezza.

Alla luce di ciò, anche per limitare il più possibile i controlli, Dayco ha adottato le misure di sicurezza più idonee per proteggere i propri sistemi informatici dall'eventuale utilizzo non accorto della navigazione su Internet da parte dei lavoratori.

In particolar modo, ha:

- individuato le categorie di siti considerate non correlate con la prestazione lavorativa;
- impedito la navigazione su detti siti attraverso l'utilizzo di un sistema di filtri sulla navigazione e sulle attività ritenute potenzialmente dannose;
- predisposto nel tempo la conservazione dei dati strettamente limitati al perseguimento di finalità organizzative, produttive e di sicurezza.

L'utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e, più in generale, delle modalità con cui opera. Il prelievo (*download*) o la consultazione *online* anche in *streaming* di immagini, file musicali, file video non è consentito. Il prelievo (*download*) o la consultazione

online anche in *streaming* di immagini, file musicali, file video e in ogni caso di grandi quantità di dati per scopi lavorativi che possono compromettere le performance della rete, devono essere precedentemente concordate con gli addetti dei sistemi informativi di Dayco.

All'utente, pertanto, non è concesso di:

- servirsi o dar modo ad altri di servirsi della postazione di accesso ad Internet per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalle norme vigenti;
- utilizzare sistemi di *file sharing*, *podcasting*, *web casting*, se non per scopi connessi con l'attività lavorativa;
- utilizzare qualsiasi genere di social media, social network e/o forum, ad eccezione di quelli appositamente predisposti e autorizzati dal Titolare del trattamento;
- utilizzare *Internet Provider* diversi da quello predefinito da Dayco e connettere la propria postazione di lavoro aziendale alle reti di tali *Provider* con sistemi di connessione diversi da quello centralizzato (ad es., attraverso *modem*, *internet key*, ecc.). Eventuali necessità devono essere appositamente richieste per iscritto agli addetti dei sistemi informativi di Dayco. È comunque possibile utilizzare *Internet Provider* diversi da quello predefinito da Dayco esclusivamente quando ci si trovi in strutture differenti da quelle di Dayco (ad es., casa, albergo, etc.), purché, nel caso in cui si debba accedere ai dati aziendali, ciò avvenga esclusivamente attraverso l'utilizzo di tecnologie di connessione sicure (ad es., le VPN, certificati HTTPS, ecc.);
- usare la rete in modo difforme da quanto previsto dalla presente Policy e da tutti gli altri regolamenti interni aziendali, nonché ancor prima dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete Internet.

Dayco si riserva fin da ora il diritto di memorizzare in appositi registri automatizzati (*log file*) i *link* delle pagine accedute attraverso la rete Internet, nelle forme e secondo le modalità esplicitate di seguito nella presente Policy ai paragrafi 4.0 ("*Monitoraggio e controlli*") e 4.1 ("*Monitoraggio e controllo delle attività degli Amministratori di Sistema*").

.13 PROTEZIONE ANTIVIRUS

Ogni lavoratore deve tenere comportamenti atti alla collaborazione fattiva con Dayco per ridurre al minimo il rischio di attacchi ai sistemi informatici aziendali attraverso *software* malevoli (ad es., *worm*, *virus*, *trojan*, ecc.) e, più in generale, attraverso l'azione di programmi di cui all'art. 615-*quinquies* del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.

Ogni utente, pertanto, è tenuto a:

- segnalare all'Amministratore di Sistema il non regolare funzionamento del *software* antivirus installato;
- segnalare prontamente all'Amministratore di Sistema il caso in cui il *software* antivirus non riesca automaticamente ad eliminare la minaccia dai sistemi aziendali;
- verificare con il *software* antivirus, prima dell'apertura di qualsiasi *file*, ogni dispositivo (ad es., chiavette USB, DVD, CD, *hard disk* esterni, ecc.) proveniente dall'esterno della nostra struttura.

Dayco si riserva fin da ora il diritto di installare su ogni postazione di lavoro elettronica i programmi che impediscano l'installazione e la diffusione di *software* potenzialmente dannoso per la sicurezza della rete aziendale. La rimozione arbitraria di detti programmi è assolutamente vietata.

.14 UTILIZZO DI APPARATI PER LA TELEFONIA MOBILE E PER LA NAVIGAZIONE ATTRAVERSO RETE MOBILE

Relativamente agli apparati di telefonia mobile, Dayco ha in essere due modalità di utilizzo dei medesimi. A prescindere dalla modalità prescelta dal lavoratore, l'utilizzo dell'apparato e della SIM aziendale deve sempre ispirarsi ai principi di diligenza, correttezza e buona fede ed al rispetto delle norme di legge.

In relazione alla scelta operata da ciascun lavoratore ed opportunamente formalizzata ai Servizi Generali, valgono le seguenti regole:

Opzione A: utilizzo esclusivo aziendale. Ogni lavoratore che sia assegnatario di un telefono cellulare ovvero di qualsiasi dispositivo che consenta l'accesso a servizi voce e/o dati mediante rete mobile, ivi comprese anche le sole schede SIM, ha l'obbligo di utilizzare detti strumenti esclusivamente per scopi connessi all'attività lavorativa e alle motivazioni che hanno spinto Dayco a questa specifica dotazione. È fatto divieto al lavoratore di utilizzare i dispositivi di telefonia mobile assegnati con questa modalità per scopi personali, considerando tali anche l'archiviazione di foto, video, messaggi e documenti personali, nonché installare sul dispositivo qualsiasi applicazione che non sia precedentemente autorizzata da Dayco.

Opzione B: doppio utilizzo (aziendale e privato). Ogni lavoratore che abbia scelto un utilizzo misto del telefono cellulare ha diritto di utilizzare il dispositivo mobile assegnato anche per uso personale nei limiti della modalità prescelta.

Al momento della restituzione o in caso di cessazione del rapporto di lavoro per qualsivoglia ragione, l'utilizzatore ha l'obbligo di cancellare qualsiasi informazione di natura personale registrata all'interno del dispositivo, ivi compresi, a titolo esemplificativo e non esaustivo, nomi

e cognomi, numeri di telefono, messaggi, fotografie, video e quant'altro sia conservato al suo interno. In mancanza saranno gli addetti della struttura di Dayco che gestisce i dispositivi ad effettuare – senza preavviso e alla prima occasione utile – questa operazione, operando attraverso procedimenti di *hard reset* e senza mai accedere ai dati contenuti all'interno dei dispositivi.

In caso di furto o smarrimento, l'utente assegnatario del telefono cellulare ha l'obbligo d'informare tempestivamente il proprio diretto responsabile di funzione e gli addetti ai sistemi informativi di Dayco, nonché di denunciare tempestivamente l'accaduto alle Forze dell'Ordine, fornendo a Dayco, entro 24 ore dall'evento, la copia dell'atto di denuncia. Atto di denuncia che deve necessariamente contenere anche la marca, il modello e il codice IMEI del dispositivo.

Per tutte le opzioni, al fine di evitare qualsivoglia accesso e utilizzo indesiderato o illecito, è fatto obbligo che ciascun dispositivo venga protetto dal suo utilizzatore quantomeno attraverso un codice PIN ovvero una parola chiave (*password*) che, nei limiti di quanto tecnicamente possibile, dovrà seguire le regole dettate in precedenza all'interno del paragrafo 3.2 ("*Gestione delle password*").

.15 MONITORAGGIO E CONTROLLI.

Dayco ha l'obbligo di salvaguardare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori dal punto di vista produttivo, dell'organizzazione e della sicurezza, al fine di assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati, anche per prevenire utilizzi indebiti che possano essere fonte di responsabilità.

Per far ciò, Dayco si avvale di sistemi informatici di controllo volti a verificare il corretto funzionamento ed utilizzo degli strumenti elettronici.

Pertanto, Dayco si riserva il diritto di controllare in qualunque momento e in maniera occasionale e/o discontinua il corretto utilizzo degli strumenti di lavoro, implementando, però, ogni misura tecnologica volta a minimizzare il più possibile l'uso di dati identificativi dei lavoratori, nei modi e con i limiti di seguito meglio esplicitati. Tali controlli verranno impiegati anche per un'eventuale verifica delle condotte del lavoratore, ottemperando al dettato dell'art. 4 della Legge n. 300 del 20 maggio 1970 - "Statuto dei lavoratori" e delle norme ad esso collegate.

Le attività sull'uso del servizio di accesso ad Internet vengono automaticamente registrate in forma elettronica attraverso i c.d. "*log* di sistema" tenuti dal *Provider* dei servizi Internet. Questi sistemi *software* sono programmati e configurati in modo da cancellare periodicamente e automaticamente, attraverso procedure di sovraregistrazione, i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia più necessaria. Questi dati, comunque, saranno conservati per un periodo non superiore a 3 (tre) mesi.

Come regola generale, inoltre, in assenza di particolari e ulteriori esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti informatici del lavoratore sarà possibile solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato per finalità lavorative e/o di continuità operativa dell'azienda;
- all'indispensabilità del dato per l'esercizio o la difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire dette finalità e sarà effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità precedentemente esplicitati.

Ai sensi del Provvedimento del Garante per la protezione dei dati personali "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" del 27 novembre 2008 (di seguito "**Provvedimento sugli Amministratori di Sistema**") e sue successive integrazioni e modificazioni, Dayco rende noto che l'elenco aggiornato contenente il nominativo dei soggetti qualificati come "Amministratore di sistema" è richiedibile al Titolare del trattamento, così come identificati all'interno dell'Informativa Privacy allegata alla presente Policy.

Ogni lavoratore potrà far valere i propri diritti sanciti dall'art. 15 ("*Diritto di accesso dell'interessato*"), dall'art. 16 ("*Diritto di rettifica*"), dall'art. 17 ("*Diritto alla cancellazione – Diritto all'oblio*"), dall'art. 18 ("*Diritto di limitazione di trattamento*"), dall'art 20 ("*Diritto alla portabilità dei dati*") e dagli altri diritti previsti all'interno del Regolamento ed esplicitati nell'Informativa Privacy presente nella Policy, rivolgendo una specifica richiesta scritta al Titolare del trattamento: Dayco Europe S.r.l., Via Papa Leone XIII n. 45, Chieti (CH), ovvero mandando una email all'indirizzo di posta elettronica certificata: privacy@PEC.daycoeurope.com.

.16 MONITORAGGIO E CONTROLLO DELLE ATTIVITÀ DEGLI AMMINISTRATORI DI SISTEMA

Per quanto attiene le postazioni di lavoro informatiche dei dipendenti designati come Amministratore di sistema, oltre a tutto quanto finora evidenziato, anche in questo caso saranno adottati idonei sistemi di registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici.

Le registrazioni (*access log*) avranno le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità in ragione dello scopo di controllo per cui sono richieste e ricomprenderanno, inoltre, i riferimenti temporali e la descrizione dell'evento che le ha generate per un periodo che sia congruo, comunque non inferiore a 6 (sei) mesi, come per legge.

Così come previsto dal Provvedimento sugli Amministratori di Sistema e suoi allegati, occorre infine rendere noto che, ai fini dell'assolvimento dell'obbligo di registrazione degli accessi logici da parte degli Amministratori di Sistema, saranno registrati gli accessi degli utenti che hanno privilegi amministrativi ai sistemi informatici aziendali.

.17 GRADUAZIONE DEI CONTROLLI

Nel caso si renda necessario effettuare dei controlli sull'uso degli strumenti elettronici, saranno rispettati i principi di pertinenza e non eccedenza degli stessi, onde evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure dei soggetti esterni che ricevono o inviano comunicazioni elettroniche.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, Dayco, pertanto, metterà in atto le opportune misure tecniche e tecnologiche volte alla verifica dei comportamenti anomali secondo la seguente procedura:

- sarà preferito, per quanto possibile, un controllo preliminare su dati aggregati e anonimi, riferiti all'intera struttura lavorativa o a sue specifiche aree;
- il controllo anonimo si concluderà con un avviso generalizzato relativo al rilevato utilizzo anomalo degli strumenti elettronici aziendali e con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite attraverso la presente Policy e le ulteriori normative aziendali interne. L'avviso potrà anche essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia;
- in caso del perdurare delle anomalie, sarà ritenuto giustificato porre in essere gli opportuni controlli su base individuale, che, ad ogni modo, non potranno essere prolungati oltre il tempo ragionevole per lo svolgimento dell'accertamento, ovvero essere costanti e indiscriminati.

.18 SOSPENSIONE CAUTELARE DEL LAVORATORE E CESSAZIONE DEL RAPPORTO DI LAVORO

Come più volte specificato all'interno di questa Policy, l'*account* di posta elettronica del dipendente e il suo *personal computer* (PC) aziendale sono strumenti di lavoro. Pertanto, le informazioni presenti al loro interno devono essere sempre considerate e trattate come lavorative e non personali. Pertanto, in caso di sospensione cautelare del lavoratore, Dayco si riserva fin da ora il diritto di poter eventualmente accedere in qualunque momento alle informazioni e ai dati presenti all'interno degli *account* di posta elettronica e/o del *personal computer* (PC) aziendale, sia fisso che portatile, per finalità di salvaguardia dei propri diritti in sede giudiziaria. Detta

attività sarà sempre ispirata al principio di proporzionalità e non eccedenza rispetto allo scopo di verifica dell'eventuale inadempimento contrattuale del lavoratore.

Inoltre, con riferimento ai trattamenti effettuati sulla posta elettronica aziendale del dipendente dopo la cessazione del rapporto di lavoro, in conformità con i principi in materia di protezione dei dati personali, gli *account* riconducibili a persone identificate o identificabili saranno rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informare i terzi e a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del Titolare del trattamento.

Allo scopo, in caso di cessazione del rapporto di lavoro, Dayco provvederà entro 72 ore alla disattivazione degli *account* e alla contestuale adozione di sistemi automatici volti ad informare i terzi in merito agli indirizzi alternativi riferiti all'attività professionale del Titolare del trattamento. Inoltre, salvo i casi in cui la conservazione delle informazioni e dei dati sia necessaria per la continuativa dell'attività lavorativa del Titolare e/o per la finalità di tutela dei propri diritti in sede giudiziaria, Dayco provvederà alla completa cancellazione dell'*account* entro 6 (sei) mesi dalla cessazione del rapporto di lavoro.

Infine, in caso di sospensione cautelare del dipendente e/o di cessazione del rapporto di lavoro, è fatto divieto ad ogni dipendente di sottrarre e/o cancellare per qualsivoglia ragione la documentazione lavorativa dagli *account* di posta elettronica o dal *personal computer* (PC) aziendale.

.19 NON OSSERVANZA DELLA NORMATIVA AZIENDALE

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con la presente Policy. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari previsti dal vigente CCNL, nonché con le azioni civili e penali consentite.

Per tutti gli altri utenti (come, ad esempio, consulenti, collaboratori, fornitori, *business partner*, ecc.), il mancato rispetto e/o la violazione delle regole sopra ricordate è perseguibile con le azioni civili e penali consentite.

INFORMATIVA PRIVACY

Dipendenti Dayco Europe S.r.l.

Informativa ai sensi dell'art. 13 del
Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio

.20 INFORMATIVA PRIVACY

Gentile Dipendente,

Dayco Europe S.r.l. (di seguito "**Dayco**" o "**Società**"), in qualità di Titolare del trattamento, desidera informarLa che, ai sensi dell'art. 13 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito "**Regolamento Europeo**" o "**GDPR**"), ha necessità di procedere al trattamento dei dati personali da Lei forniti attraverso la stipula del contratto di lavoro (di seguito "**Contratto**") e durante l'esecuzione giornaliera delle Sue mansioni lavorative nel rispetto della normativa vigente e secondo quanto di seguito riportato.

1. TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è Dayco Europe S.r.l., in persona del Presidente del Consiglio di Amministrazione, domiciliato presso la sede legale di Via Papa Leone XIII n. 45, Chieti (CH) (di seguito "**Titolare del trattamento**" o "**Titolare**").

2. OGGETTO DEL TRATTAMENTO

Il Titolare tratta i seguenti dati personali (in seguito "Dati"):

- identificativi: ossia i dati personali che permettono l'identificazione diretta dell'interessato (a titolo meramente esemplificativo e non esaustivo: nome, cognome, estremi anagrafici, indirizzo, componenti del nucleo familiare ed eventuali familiari a carico, telefono, e-mail, riferimenti bancari ecc.);
- relativi alla salute: ossia i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al Suo stato di salute;
- dati eventualmente acquisiti per garantire l'accesso sia alle sedi che al sistema informativo aziendale, nel rispetto dei limiti di legge;
- relativi al rapporto giuridico attivato con la nostra società (a titolo meramente esemplificativo e non esaustivo: rapporto di lavoro subordinato, ecc.);

- immagini fotografiche e immagini raccolte tramite impianti di videoregistrazione, regolarmente segnalati, autorizzati e utilizzati nel rispetto di quanto previsto dallo Statuto dei Lavoratori;

- dati eventualmente acquisiti a mezzo specifiche applicazioni e/o software sviluppati e/o comunque utilizzati dal Titolare per finalità operative.

Il Titolare potrebbe, inoltre, dover venire a conoscenza di dati "giudiziari" ex art. 10 GDPR e di altre categorie particolari di dati personali ex art. 9 GDPR (ad es. l'adesione a partiti politici, dati relativi a convinzioni religiose, origini razziali o etniche, ecc.), con l'unico scopo di eseguire le azioni inerenti le tipologie di trattamenti sotto descritti e comunque derivanti da obblighi di legge.

I Dati sono forniti dall'interessato direttamente ovvero possono essere raccolti presso terzi autonomi titolari e/o responsabili del trattamento (a titolo meramente esemplificativo: agenzie interinali, head hunter, registri, elenchi o banche dati pubbliche, ovvero società, italiane o estere, che prestano servizi in favore e per conto del Titolare, nonché eventuali società controllanti, controllate e/o in qualche modo collegate alla Dayco Europe S.r.l.).

Il Titolare potrebbe altresì avere necessità di acquisire anche dati personali dei familiari (es. nome, cognome, data di nascita e grado di parentela, permessi per assistenza, ecc.) dell'interessato, al fine di eseguire i trattamenti richiamati nella presente informativa e comunque per il rispetto di qualsivoglia obbligo di legge.

Si precisa che eventuali variazioni dei Dati da Lei direttamente comunicati dovranno essere a Sua cura tempestivamente trasmesse al Titolare.

3. FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO

In considerazione del rapporto di lavoro esistente tra Lei e Dayco, la base giuridica su cui si fonda il trattamento dei Suoi dati personali è la stipulazione del Contratto attivato con la nostra società e/o il Suo coinvolgimento nelle attività di ricerca e selezione del nostro personale, oltre che il legittimo interesse del Titolare a trattare i Dati per determinate finalità e il Suo specifico ed espresso consenso - laddove necessario -.

Pertanto, i dati personali ed eventualmente anche quelli appartenenti a categorie particolari di Dati trattati da Dayco sono esclusivamente quelli da Lei forniti in occasione della sottoscrizione del Contratto o durante l'espletamento di tutte le formalità sia prodromiche che successive all'instaurazione del rapporto di lavoro, così come quelli utili per l'esecuzione giornaliera delle Sue mansioni lavorative.

Pertanto, i Suoi dati personali verranno trattati esclusivamente per:

A) permettere l'instaurazione, la gestione, l'esecuzione e la cessazione del rapporto di lavoro e dei conseguenti adempimenti derivanti da obblighi di legge, dai contratti collettivi anche aziendali, da obblighi amministrativi, contributivi, previdenziali, assistenziali, contabili, fiscali,

finanziari, assicurativi, formativi, di igiene e tutela della salute e sicurezza sui luoghi di lavoro, nonché dagli adempimenti derivanti dalle attività in materia di welfare e di sicurezza dei sistemi informatici, delle reti e delle informazioni aziendali.

B) facilitare la comunicazione e i rapporti interpersonali e lavorativi tra i colleghi e/o altri soggetti esterni alla Società, attraverso l'inserimento nella intranet aziendale, a mero titolo esemplificativo e non esaustivo, della sua foto, della data di instaurazione del rapporto di lavoro, di una breve descrizione delle sue esperienze pregresse e, più in generale, di dati presenti in rubriche a tema.

C) consentire la condivisione di informazioni rilevanti ai fini amministrativi interni all'interno del Gruppo Dayco.

D) garantire la sicurezza del personale dipendente e dei soggetti che accedono ai locali (e relative pertinenze) del Titolare (ad es. per ragioni di salute e sicurezza sui luoghi di lavoro), oltre che protezione dei beni e del patrimonio aziendale (es. videosorveglianza) rispetto a possibili aggressioni, furti, rapine, danneggiamenti o atti di vandalismo.

Il trattamento dei Suoi Dati è realizzato per mezzo delle operazioni indicate all'art. 4 n. 2) GDPR e precisamente: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione dei dati.

I Suoi Dati sono sottoposti a trattamento sia cartaceo che elettronico e/o automatizzato, nonché inseriti nelle pertinenti banche dati aziendali (lavoratori subordinati, collaboratori, stagisti, amministrazione, ecc.) cui potranno accedere e, quindi, venirne a conoscenza, gli addetti espressamente designati dal Titolare quali i dipendenti autorizzati al trattamento, i responsabili e sub-responsabili del trattamento, gli amministratori di sistema (interni ed esterni), i quali potranno effettuare operazioni di consultazione, utilizzo, elaborazione, raffronto ed ogni altra opportuna operazione anche automatizzata entro i limiti delle nomine loro conferite e nel rispetto delle disposizioni di legge necessarie a garantire, tra l'altro, la riservatezza e la sicurezza dei dati nonché l'esattezza, l'aggiornamento e la pertinenza dei dati nel rispetto alle finalità dichiarate.

4. PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

Il Titolare del trattamento intende conservare i Suoi dati personali per un arco di tempo non superiore rispetto a quello necessario per il conseguimento delle finalità per i quali sono raccolti e trattati.

In quest'ottica, Dayco dovrà necessariamente trattare i Suoi dati personali per tutta la durata del rapporto di lavoro. Pertanto, non potendo determinare con precisione il periodo di conservazione dei Suoi dati personali, Dayco si impegna fin da ora ad ispirare il trattamento dei Suoi dati personali ai principi di adeguatezza, pertinenza e minimizzazione dei dati, così come richiesto dal Regolamento Europeo, verificando annualmente la necessità della loro conservazione.

Successivamente alla conclusione del rapporto di lavoro, inoltre, Dayco dovrà conservare alcuni Suoi dati personali per l'espletamento di tutti gli obblighi di legge e per le finalità amministrative derivanti da questi obblighi. In questo caso, fermo restando i principi poc'anzi elencati, il Titolare del trattamento conserverà questi dati per un periodo massimo di 10 anni, al fine di poter far fronte alle suddette eventuali necessità o a richieste da parte delle autorità di controllo.

Ciò, fatto salvo il caso in cui avremo bisogno di mantenere tali dati per adempire ad obblighi normativi, oppure per accertare, esercitare o difendere concretamente un nostro diritto in sede giudiziaria.

Per maggiori informazioni sulla politica di conservazione dei Dati, è possibile consultare la policy implementata dalla Società richiedendone copia all'ufficio risorse umane.

5. CATEGORIE DI DESTINATARI DEI DATI PERSONALI

I dati trattati non saranno oggetto di diffusione a terzi. Possono comunque venire a conoscenza dei Suoi dati, in relazione alle finalità di trattamento precedentemente esposte:

- i soggetti che possono accedere ai dati in forza di disposizione di legge previste dal diritto dell'Unione Europea o da quello dello Stato membro cui è soggetto il Titolare del trattamento;
- il nostro personale dipendente, purché sia precedentemente designato come soggetto autorizzato al trattamento dal Titolare del trattamento a norma dell'art. 29 del Regolamento Europeo, come Amministratore di Sistema e/o soggetto munito di specifiche funzioni e compiti *ex* art. 2-*quaterdecies* D.Lgs. n. 196/2003;
- altre società (controllanti, controllate e/o collegate) facenti parte del nostro gruppo imprenditoriale, per finalità amministrative interne o sulla base di specifici accordi sottoscritti ai sensi degli artt. 26 e 28 GDPR;
- soggetti che svolgono, all'interno dei confini dell'Unione Europea, in totale autonomia, come distinti Titolari del trattamento, ovvero in qualità di Responsabili o sub-Responsabili del trattamento all'uopo nominati da Dayco ai sensi dell'art. 29 del Regolamento Europeo, finalità ausiliarie alle attività e ai servizi di cui al paragrafo 2., ovvero istituti bancari e assicurativi, studi legali e notarili, società e consulenti fiscali, del lavoro e per la selezione, formazione e valutazione del personale, società che offrono servizi di *payroll*, casse di previdenza sociale, società che offrono servizi di welfare, medico aziendale, società di assistenza e consulenza informatica nonché progettazione e realizzazione di software e/o siti Internet, servizi postali, centri di servizio, società o consulenti incaricati di fornire servizi al Titolare del trattamento, nei limiti delle finalità per le quali sono stati raccolti.

Si precisa che l'elenco dei Responsabili del trattamento è custodito presso la sede legale del Titolare.

L'eventuale comunicazione dei Suoi dati personali, anche nel caso di Paesi extra-UE, avverrà nel pieno rispetto delle disposizioni di legge previste dal Regolamento Europeo e delle misure tecniche e organizzative predisposte dalla Società per garantire un adeguato livello di sicurezza.

6. TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI

Il Titolare del trattamento intende trasferire, per finalità amministrative interne ai sensi del "Considerando 48" del GDPR ovvero nel caso di esternalizzazione di talune attività ad altre società del Gruppo Dayco, i Suoi dati - anche particolari ex art. 9 GDPR - verso paesi terzi, e più precisamente verso gli Stati Uniti alla Capogruppo Dayco LLC o altri stati in cui operano le società del Gruppo Dayco. In tal caso, il Titolare assicura che il trasferimento dei Dati extra-UE presenti garanzie adeguate ai sensi dell'articolo 46 del Regolamento Europeo, come il caso del *Data Transfer Agreement* stipulato tra Dayco Europe S.r.l. e Dayco Products LLC, e che avverrà nel rispetto del principio di minimizzazione di cui all'art. 5 del GDPR e delle vigenti *standard contractual clauses* previste dalla Commissione Europea, in ogni caso in conformità alle disposizioni di legge applicabili in materia.

7. EVENTUALI PROCESSI DECISIONALI AUTOMATIZZATI

Il Titolare del trattamento non intende utilizzare processi decisionali automatizzati, ivi compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del Regolamento Europeo. Pertanto, il Titolare del trattamento ritiene di non dover fornire informazioni sulla logica utilizzata, nonché sull'importanza e le conseguenze per l'interessato relative a questo tipo di trattamento.

8. NATURA DEL CONFERIMENTO

Il conferimento dei Suoi dati personali per le finalità di cui ai paragrafi 3.A, 3.C e 3.D ha natura obbligatoria, in quanto la mancata autorizzazione al loro trattamento potrebbe comportare l'impossibilità per la Società di adempiere agli obblighi di legge e/o a quelli derivanti dalla gestione del rapporto contrattuale di lavoro, impedendo, di conseguenza, la sua formalizzazione ed esecuzione.

Il conferimento dei Suoi dati personali per le finalità di cui al paragrafo 3.B ha natura facoltativa, ma la mancata autorizzazione al loro trattamento, pur non impedendo l'instaurazione del rapporto di lavoro, potrebbe non consentire alla Società di facilitare la comunicazione e i rapporti interpersonali e lavorativi tra i colleghi ed eventuali soggetti esterni alla Società.

La incompleta o non veritiera comunicazione dei Suoi dati personali comporta l'impossibilità per la Società di garantire la coerenza del trattamento alle previsioni contrattuali previste, nonché la sua corrispondenza anche agli obblighi imposti dalle normative di riferimento.

9. DIRITTI DELL'INTERESSATO

In relazione al trattamento dei Suoi dati personali, ai sensi del Regolamento Europeo, Lei in qualità di interessato ha il diritto di:

- revocare il Suo consenso al trattamento in qualsiasi momento. Occorre evidenziare, tuttavia, che la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca, così come previsto dall'art. 7, comma 3, del Regolamento Europeo;

- chiedere al Titolare del trattamento l'accesso ai Suoi dati personali, così come previsto dall'art. 15 del Regolamento Europeo;

- ottenere dal Titolare del trattamento la rettifica e l'integrazione dei Suoi dati personali ritenuti inesatti, anche fornendo una semplice dichiarazione integrativa, così come previsto dall'art. 16 del Regolamento Europeo;

- ottenere dal Titolare del trattamento la cancellazione dei Suoi dati personali qualora sussista anche solo uno dei motivi previsti dall'art. 17 del Regolamento Europeo;

- ottenere dal Titolare del trattamento la limitazione del trattamento dei Suoi dati personali qualora ricorrano una delle ipotesi previste dall'art. 18 del Regolamento Europeo;

- ricevere dal Titolare del trattamento i dati personali che La riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico, nonché ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti, così come previsto dall'art. 20 del Regolamento Europeo;

- opporsi in qualsiasi momento, per motivi connessi alla Sua situazione particolare, al trattamento dei Suoi dati personali svolto ai sensi dell'art. 6, paragrafo 1, lettere *e)* o *f)*, compresa la profilazione sulla base di tali disposizioni, così come previsto dall'art. 21 del Regolamento Europeo;

- non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che producano effetti giuridici che La riguardino o che incidano significativamente sulla Sua persona, qualora non abbia preventivamente ed esplicitamente acconsentito, così come previsto dall'art. 22 del Regolamento Europeo. A mero titolo esemplificativo e non esaustivo, rientra in questa categoria qualsiasi forma di trattamento automatizzato di dati personali teso ad analizzare o prevedere aspetti riguardanti le scelte di consumo e di acquisto, la situazione economica, gli interessi, l'affidabilità, il comportamento;

- proporre reclamo ad un'autorità di controllo, qualora ritenga che il trattamento che La riguarda violi il Regolamento Europeo. Il reclamo può essere proposto nello Stato membro in cui risiede abitualmente, lavora oppure nel luogo ove si è verificata la presunta violazione, così come previsto dall'art. 77 del Regolamento Europeo.

Per esercitare ciascuno dei Suoi diritti, Lei può contattare il Titolare del trattamento, nella persona del Presidente del Consiglio di Amministrazione, indirizzando una comunicazione presso la sede legale di Via Papa Leone XIII n. 45, Chieti (CH), oppure inviando una e-mail all'indirizzo di posta elettronica certificata: privacy@PEC.daycoeurope.com.