Legittimo Interesse per alcuni trattamenti dati dei dipendenti

Banca di Credito Cooperativo di Buccino e dei Comuni Cilentani Società Cooperativa
Sede Legale e Direzione Generale: 84043 Agropoli (SA) – Via S. Pio X n.30/32
Tel.: +39 0974 821011 – Fax 0974 821104
Email: segreteria@comunicilentani.bcc.it - Sito web: www.buccinocomunicilentani.it
Pec: segreteria@pec.bcccomunicilentani.it - Swift ICRAITRRTM0

Iscrizione Albo Cooperative n.A162403 - Iscrizione Albo Imprese Creditizie Cod. Abi 07066
Società partecipante al Gruppo IVA Gruppo Bancario Cooperativo Iccrea, Partita IVA 15240741007
Registro Imprese C.F. 03685090650 - CCIAA REA PD n. SA-313216 - Cod. SDI 9GHPHLV
Aderente al Fondo di Garanzia degli Obbligazionisti del Credito Cooperativo (FGO), al Fondo di Garanzia dei Depositanti del Credito Cooperativo (FGD), al Fondo Nazionale di Garanzia (FNG)

Sommario

Introduzione

Le Società, le Banche di Credito Cooperativo, le Casse Rurali ed Artigiane (nel seguito anche 'Aziende') che sono parte del Gruppo Bancario Cooperativo Iccrea (nel seguito 'Gruppo', 'ICCREA'), svolgono trattamenti di dati personali dei propri lavoratori (nel seguito anche 'dipendenti') per una pluralità di esigenze, le cui basi legali ai sensi dell'Art.6 del Reg. Europeo 2016/679 (GDPR) trovano in gran parte fondamento sia nel rispetto di obblighi derivanti da leggi e regolamenti nazionali ed Europei (GDPR Art. 6(1)(c)), che sulla necessità di adempiere ad obblighi contrattuali (incluse le fasi pre-contrattuali) nei riguardi del dipendente stesso (GDPR Art. 6(1)(b)).

Per altri casi di trattamento le suddette due tipologie di basi legali non risultano applicabili (assenza di una legge o di un presupposto contrattuale che renda necessario quei trattamenti) né tanto meno può aver senso ricorrere ad altre basi legali quali la salvaguardia di interessi vitali (GDPR Art. 6(1)(d)) o l'esecuzione di un compito di interesse pubblico (GDPR Art. 6(1)(e)).

Pertanto, in tali casi occorre individuare la base legale tra il consenso del dipendente (GDPR Art. 6(1)(a)) ed il legittimo interesse dell'Azienda o di terzi (GDPR Art. 6(1)(f)) operando scelte nel rispetto del principio fondante del GDPR, e dunque la protezione dei diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali (GDPR Art. 1(2)).

I casi di attività di trattamento in oggetto alla presente analisi sono i seguenti:

1) Amministrazione e direzione aziendale;
2) Sicurezza delle reti e delle Informazioni.

Nei successivi paragrafi è documentata l'analisi svolta ai fini del bilanciamento degli interessi, prevista per l'eventuale adozione del legittimo interesse, come base legale ai sensi del GDPR Art. 6 (1)(f), dell'Azienda e di Terzi (ossia la Capogruppo e tutte le società del Gruppo). Tale attività è stata condotta tenendo presenti le apposte indicazioni rinvenibili nel GDPR nonché le specifiche opinioni e lavori svolti dal WP 29 (gruppo di lavoro istituito in base all'art 29 della direttiva Europea 95/46/EC, ora EDPB - European Data Protection Board, istituito con l'Art 68 GDPR).

Laddove l'esito dell'analisi di bilanciamento non fornisca un oggettivo riscontro a favore del Legittimo Interesse per l'Azienda ed i Terzi indicati, occorre optare per il Consenso come base legale per i suddetti casi di trattamento.

1) Amministrazione e direzione aziendale

Contesto

La specifica Azienda, la Capogruppo e le altre società del Gruppo, hanno l'esigenza di trasmettere e trattare all'interno del Gruppo i dati personali del lavoratore per:

A. le finalità amministrative interne del Gruppo stesso, inclusa la gestione dei processi integrati in contesto Gruppo, quali – ad esempio – il conseguimento di economie di scala;
B. le finalità e le conseguenti attività connesse all'azione di direzione e coordinamento della Capogruppo (es. governo societario, pianificazione strategica, governo dei rischi e sistema dei controlli interni, politiche creditizie e connessi profili di rischio, gestione finanziaria, attività commerciale e distributiva,

amministrazione e segnalazione di vigilanza, gestione degli aspetti fiscali, modello di organizzazione, gestione e sviluppo delle risorse umane e mobilità infragruppo, sistemi informativi e attività legali);

C. la promozione di eventi e iniziative dell'Azienda e delle società del Gruppo rivolte ai dipendenti, attraverso l'utilizzo della posta elettronica aziendale e della intranet aziendale.

Valutazione interessi dell'Azienda e dei Terzi

Necessità del trattamento

L'Azienda ed i Terzi non possono prescindere dal condurre attività di amministrazione e direzione per la gestione delle attività societarie per le quali sono necessari trattamenti di dati personali riferiti a dipendenti. In tal senso si era già espressa la normativa italiana in materia di protezione dei dati personali vigente pre-GDPR, laddove nell'Art. 24 del D. Lgs. 196/03, ove erano elencati i casi di esclusione del Consenso, il punto i-ter del comma 1 (introdotto nel 2011 all'epoca del Governo Monti) riportava:

> *"i-ter) con esclusione della diffusione e fatto salvo quanto previsto dall'articolo 130 del presente codice, riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'articolo 2359 del codice civile ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrativo contabili, come definite all'articolo 34, comma 1-ter, e purché queste finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13.";*

La definizione di finalità 'amministrativo contabili' di cui al richiamato Art. 34 comma 1-ter del previgente D. Lgs. 196/03 è la seguente:

> "*Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo - contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale - assistenziale, di salute, igiene e sicurezza sul lavoro*".

Medesimi concetti sono ripresi ed espressi nel considerando (48) del GDPR:

> *"I titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti. Sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in un paese terzo.*

Da notare che in base a quanto previsto nel Contratto di Coesione che regolamenta il Gruppo, in particolare: Art. 5.10 e Art. 4, lett. e) punto (i), sono espressamente previste attività infragruppo ai fini della gestione e sviluppo delle risorse umane e mobilità infragruppo che non possono prescindere dalla comunicazione dei dati personali riferiti al dipendente di volta in volta necessari per il caso specifico. Da notare che rientra a pieno diritto in questa casistica anche quanto si predispone (vedi sub caso C indicato precedentemente) per promuovere nel Gruppo, anche con la partecipazione ad appositi eventi e corsi formativi:

- la crescita professionale,

- la conoscenza dei prodotti e servizi che costituiscono le basi del business delle società del Gruppo,

- le occasioni per promuovere la reciproca conoscenza e cooperazione tra i lavoratori delle società del Gruppo,

in quanto tutto ciò è base indispensabile e volano per mantenere e migliorare la quota di mercato Iccrea: per tali motivi il Gruppo ha investito ed intende continuare ad investire sempre più in futuro per simili iniziative.

Proporzionalità ed effetti del trattamento, circolazione dei dati

L'Azienda ed i Terzi sono già obbligati ad applicare il principio di 'Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita di cui all'Art. 25 GDPR, per cui le circolazioni dei dati infragruppo in ogni caso riguardano solo i dati strettamente necessari, la comunicazione è limitata ai soli soggetti che sono tenuti, all'interno del Gruppo, a riceverli per condurre le attività loro assegnate, ed a conservarli in una forma che consenta l'identificazione del lavoratore solo per il tempo necessario per il conseguimento delle finalità poste alla base della comunicazione stessa. In nessun caso l'Azienda ed i Terzi, in considerazione dei sub punti A, B e C indicati in Contesto, possono voler effettuare attività ed applicare ulteriori misure anche su dati eccedenti a quanto strettamente necessario. Gli effetti del trattamento sono esclusivamente quelli derivanti dalle finalità di cui ai già richiamati sub punti A, B e C, e, peraltro, nel contesto delle attività condotte nelle società del Gruppo, i lavoratori in qualità di Interessati, possono ben ragionevolmente attendersi che abbia luogo un trattamento dei loro dati per le finalità sopra indicate.

In nessun caso, per quanto qui in esame, sono attuate né previste attività di trattamento automatizzato sui dati del lavoratore, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Trasparenza nei confronti degli Interessati

Nell'Informativa ex Artt. 13 e 14 GDPR che deve essere resa ai dipendenti al momento del loro ingresso in Azienda, o successivamente nel caso intervengano aggiornamenti in merito ai loro trattamenti di dati personali, saranno indicati specificamente e separatamente quei contesti di finalità-trattamenti per i quali l'Azienda ed i Terzi si avvalgono del Legittimo Interesse come base legale ai sensi dell'Art. 6 GDPR.

Pertanto, ciò comporterà:

1) in primo luogo, l'aggiornamento del Registro Attività di trattamento delle Aziende che si avvalgono del Legittimo Interesse come base legale per determinati trattamenti di dati personali dei lavoratori
2) l'aggiornamento dell'attuale modello di Informativa per i dipendenti, che verrà utilizzato al momento dell'accensione di un nuovo rapporto 'datore di lavoro – lavoratore' all'interno del Gruppo, e
3) la definizione di una strategia operativa affinché tutti coloro che sono già dipendenti di società del Gruppo, ricevano in modo documentato la Informativa aggiornata entro un prefissato periodo di tempo.

Per quanto concerne l'esercizio dei diritti dei dipendenti in qualità di Interessati, in particolare, il diritto di opposizione di cui all'Art. 21 GDPR è già menzionato nell'attuale modello di Informativa per i dipendenti.

Qualora l'Azienda o uno dei Terzi riceva una richiesta di opposizione ad un trattamento basato sul Legittimo Interesse, coerentemente con quanto previsto nel comma 1 dell'Art. 21 GDPR:

4) dovrà essere predisposta una Nota, da comunicare formalmente al richiedente, redatta sulla base di questo documento di bilanciamento di interesse e tenendo presente il caso specifico oggetto di opposizione, onde dimostrare *"l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato".*

Tempi di conservazione ed esattezza del dato

L'Azienda ed i Terzi conserveranno i dati dei dipendenti in relazione ai sub punti A. B. e C. elencati in Contesto osservando la tempistica di volta in volta applicabile al singolo processo amministrativo che implica la circolazione dei dati personali in oggetto, tipicamente si osserva il limite dei 10 anni, o tempi inferiori o superiori se dettati dal rispetto della normativa nazionale o comunitaria applicabile, di apposite direttive da parte di Banca Italia o autorità internazionali competenti (es. European Banking Authority), fatta salva l'esigenza di conservare i dati in caso di accertamento, esercizio o difesa di un diritto in sede giudiziaria, dell'Azienda e di Terzi.

Per quanto concerne l'esattezza dei dati, questi sono trattati per finalità amministrativo contabili e dunque sono acquisiti e trattati tramite l'utilizzo di appositi sistemi, così da rendere minimo il rischio di circolare dati potenzialmente errati. Resta sempre salvo il diritto di rettifica ex Art. 16 GDPR.

Misure di sicurezza

I dati oggetto di circolazione sono trattati tramite i sistemi informativi e di comunicazione aziendale per i quali sono adottate misure di sicurezza di livello commensurato al rischio tenendo presente il contesto bancario e dunque in osservanza anche delle prescrizioni di sicurezza emanate dalle Autorità competenti (in particolare Banca d'Italia e EBA).

Le misure applicate a tali sistemi sono mantenute aggiornate in funzione del progresso tecnologico ed in base alle risultanze di apposite verifiche tecniche (vulnerability assessment, penetration test, …) e di processo (verifiche periodiche in accordo a normativa specifica del settore bancario in ottica di quanto previsto dall'Art. 32 GDPR).

Tali verifiche sono condotte sotto la responsabilità dall'Azienda o direttamente della Capogruppo, a seconda che il sistema informativo o processo sia di gestione locale (sfera di responsabilità della singola Azienda) oppure di gruppo (sfera di responsabilità della Capogruppo).

Valutazione interessi, diritti e libertà fondamentali degli Interessati

Riguardo la possibilità che i soggetti non si aspettino ragionevolmente il trattamento in oggetto

Il personale che opera nell'Aziende del Gruppo è consapevole dell'appartenenza di queste al Gruppo, e di norma prende parte, nell'ambito delle proprie attività lavorative, a diversi processi di lavoro che comportano trasferimento di informazioni infragruppo.

Sin dalla fase di selezione del Personale, viene rappresentato che l'Azienda è parte del Gruppo e che esistono varie funzioni centralizzate che svolgono attività a livello di Capogruppo ed a beneficio delle Aziende aderenti, sia per esigenze organizzative e di efficientamento sia per rispettare la normativa bancaria che richiede la presenza di processi svolti a livello di Gruppo e non di singola Azienda.

Inoltre, come indicato precedentemente alla sezione 'Trasparenza nei confronti dell'interessato', e qui riportato per comodità di lettura, sarà curato:

1) l'aggiornamento dell'attuale modello di Informativa per i dipendenti, che verrà utilizzato al momento dell'accensione di un nuovo rapporto 'datore di lavoro – lavoratore' all'interno del Gruppo, e
2) la definizione di una strategia operativa affinché tutti coloro che sono già dipendenti di società del Gruppo, ricevano in modo documentato la Informativa aggiornata entro un prefissato periodo di tempo

Pertanto, non risultano elementi che possano far considerare, ad un dipendente della Azienda, inaspettato o non prevedibile una circolazione dati a livello di Gruppo per i casi A, B e C indicati in Contesto.

Presenza di eventuali dati connaturati da particolari caratteristiche di criticità

I dati oggetto del presente trattamento sono tutti quelli correntemente utilizzati in trattamenti effettuati per finalità amministrativo – contabili, e dunque connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati, in particolare, le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale - assistenziale, di salute, igiene e sicurezza sul lavoro.

Pertanto, tra tali dati potranno essere presenti dati particolari del tipo:

- abilità o meno per determinate attività lavorative
- lo stato e composizione di famiglia ove necessario per operare specifiche contribuzioni previste dalla legge
- eventuali azioni disciplinari intraprese dall'Azienda
- informazioni inerenti alla valutazione professione ed attitudine nel contesto dei processi di sviluppo delle risorse umane
- livelli retributivi e qualifiche professionali (CV incluso) per esigenze di contabilizzazione, direzione e strategie a livello di Gruppo
- eventuale appartenenza sindacale

Questi dati sono quelli già trattati a livello di singola Azienda e la loro natura in termini di criticità non cambia passando a livello infragruppo per le finalità amministrativo contabili sopra indicate.

In ogni caso, sarà emessa una apposita direttiva (anche tramite aggiornamento della Politica per la protezione dei dati personali) a tutto il personale impegnato in attività infragruppo allo scopo di:

5) Ulteriormente richiamare l'attenzione sull'obbligo di riservatezza per tutti i dati trattati a livello Gruppo per finalità amministrativo-contabile che in particolare comportano accesso e trattamento di dati riferiti al personale delle Aziende del Gruppo, espressamente vietandone utilizzi per scopi diversi rispetto a quelli per i quali è consentito accedervi e trattarli, a meno di espressa, specifica e motivata autorizzazione da parte del responsabile gerarchico/funzionale per motivi eccezionali, per cui i dati in oggetto devono essere trattati e rimanere riservati conformemente ad un obbligo di segreto professionale disciplinato dal diritto dell'Unione o nazionale, compreso un obbligo di segretezza previsto per legge.

Impatti del trattamento sugli interessati

I trattamenti di dati del personale in forza alle Aziende del Gruppo sono volti, come già indicato, a perseguire esclusivamente finalità amministrativo-contabili per corrispondere ad esigenze di economia di scala e per svolgere trattamenti specificamente previsti a livello di Gruppo in applicazione della normativa nazionale ed Europea nel settore bancario, per cui:

- in considerazione delle misure di sicurezza tecniche organizzative nonché delle salvaguardie che ogni Azienda del Gruppo, compresa la Capogruppo, è già tenuta a porre in essere in accordo alla Politica per la protezione dati personali di ICCREA nel rispetto della normativa in materia di protezione dati personali, e
- tenendo presenti le ulteriori cautele indicate nelle precedenti sezioni,

i rischi derivanti sotto il profilo della riservatezza, integrità e disponibilità risultano mitigati dal complesso di tali misure, salvaguardie e cautele.

Esami di altre basi legali, alternative al Legittimo Interesse

Per i trattamenti in oggetto, non si ritiene che la relativa base legale possa essere pienamente individuata nel contratto ai sensi della lettera b) comma 1 Art. 6 GDPR in quanto detto contratto non intende disciplinare aspetti che dipendono dall'organizzazione delle attività amministrative interne della singola Azienda in relazione al Gruppo.

Sono escluse per definizione le basi legali quali il Pubblico Interesse, l'Interesse vitale del singolo o di altri soggetti come anche il rispetto di una legge (lettere c), d) ed e) del comma 1 Art. 6 GDPR) in quanto evidentemente non applicabili al caso in esame.

Si intende altresì escludere il ricorso al consenso lettera a) comma 1 Art. 6 GDPR in quanto:

- non si ritiene la corretta base legale per rendere lecito un trattamento che si svolge in funzione di determinati assetti organizzativi dell'Azienda, come parte di un Gruppo, che opera nel settore bancario,
- l'analisi sopra documentata in relazione al bilanciamento tra gli interessi dell'Azienda e dei Terzi da una parte, e gli interessi, i diritti e le libertà fondamentali del lavoratore dall'altra, non evidenzia l'esistenza di rischi apprezzabili,
- il consenso del lavoratore, nel contesto di finalità amministrativo contabili non avrebbe la caratteristica di essere libero, in quanto evidentemente condizionato dal diverso rapporto di forza in essere tra datore di lavoro e lavoratore, come più volte evidenziato nei lavori del WP 29 e dell'EDPB, ed anche dalla Decisione del Garante Privacy greco, vedasi [3] in Riferimenti.

Conclusioni

L'analisi condotta e documentata nelle precedenti sezioni, consente alla Azienda ed alle Terze Parti indicate, di avvalersi del legittimo interesse ai sensi della lettera f) comma 1 Art. 6 GDPR, non riscontrando alcuna lesione degli interessi, diritti e libertà fondamentali dei lavoratori in qualità di Interessati, fermo restando per questi la facoltà di esercitare il loro diritto di opposizione ai sensi dell'Art. 21 GDPR.

Si riepilogano qui di seguito le ulteriori cautele individuate dall'analisi, che nel loro complesso le Aziende del Gruppo, Capogruppo compresa, predispongono in relazione ai trattamenti in oggetto:

1) in primo luogo, l'aggiornamento del Registro Attività di trattamento delle Aziende che si avvalgono del Legittimo Interesse come base legale per determinati trattamenti di dati personali dei lavoratori,
2) l'aggiornamento dell'attuale modello di Informativa per i dipendenti, che verrà utilizzato al momento dell'accensione di un nuovo rapporto 'datore di lavoro – lavoratore' all'interno del Gruppo,
3) la definizione di una strategia operativa affinché tutti coloro che sono già dipendenti di società del Gruppo, ricevano in modo documentato la Informativa aggiornata entro un prefissato periodo di tempo,
4) dovrà essere predisposta una Nota, da comunicare formalmente al richiedente, redatta sulla base di questo documento di bilanciamento di interesse e tenendo presente il caso specifico oggetto di opposizione, onde dimostrare *"l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato",*

5) Ulteriormente richiamare l'attenzione sull'obbligo di riservatezza per tutti i dati trattati a livello Gruppo per finalità amministrativo-contabile che in particolare comportano accesso e trattamento di dati riferiti al persone delle Aziende del Gruppo, espressamente vietandone utilizzi per scopi diversi rispetto a quelli per i quali è consentito accedervi e trattarli, a meno di espressa, specifica e motivata autorizzazione da parte del responsabile gerarchico/funzionale per motivi eccezionali, per cui i dati in oggetto devono essere trattati e rimanere riservati conformemente ad un obbligo di segreto professionale disciplinato dal diritto dell'Unione o nazionale, compreso un obbligo di segretezza previsto per legge.

2) Sicurezza delle reti e delle Informazioni

Contesto

La specifica Azienda ed il Gruppo hanno l'esigenza di trattare i dati riferiti al lavoratore in relazione al suo accesso ed utilizzo delle risorse informatiche e telematiche nonché dei sistemi informativi in uso nell'Azienda e nel Gruppo, nella misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e delle informazioni gestite nell'Azienda e nel Gruppo, da parte di appositi centri adibiti alla sicurezza informatica e all'intervento in caso di emergenza informatica e di incidenti.

Da notare che tale contesto rientra appieno in quanto delineato nel GDPR con il considerando (49):

> *" Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica."*

Valutazione interessi dell'Azienda e dei Terzi

Necessità del trattamento

Pressoché qualunque attività lavorativa condotta in un'azienda, in modo particolare poi se operante nel settore bancario, comporta il trattamento di dati personali di varie tipologie di interessati (clienti, …) tramite una pluralità di sistemi informativi nonché mezzi e dispositivi di comunicazione.

In tale contesto, tutte le aziende del Gruppo, Capogruppo compresa, devono porre in essere misure di sicurezza tecnico organizzative per garantire un livello di sicurezza adeguato tenendo "*conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*", in conformità a quanto previsto dal GDPR con:

Art 32 'Sicurezza del trattamento',

Art. 34 'Comunicazione di una violazione di dati personali all'interessato' comma 3 lettere a) e b), qualora si intenda limitare il rischio di una tale comunicazione in caso di violazione dati personali di rischio elevato,

Art 35 'Valutazione d'impatto sulla protezione dei dati qualora ricorrano le condizioni di cui ai commi 2 e 4 di tale articolo.

Inoltre, tali aziende sono tenute a porre in essere tutte le misure di sicurezza stabilite a livello nazionale ed internazionale specifiche per il settore bancario (apposito provvedimento del Garante privacy [8], la normativa PSD2, la normativa antiriciclaggio, i controlli imposti dalla Agenzie delle Entrate italiana, …).

Per tale esigenza, le aziende del Gruppo, direttamente o per il tramite di fornitori di servizi informatici, tra questi compresa l'azienda BCCSI del Gruppo (principale fornitore di servizi tecnologici in ambito ICCREA), pongono in essere misure che comportano il trattamento di dati nella misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi, a cura di organizzazioni di intervento che operano a contrasto di emergenza informatica, per la sicurezza informatica in caso di incidente, fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò include le misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica utilizzati in ambito Gruppo.

Proporzionalità ed effetti del trattamento, circolazione dei dati

Relativamente alle misure di sicurezza:

- *specificamente individuate e prescritte dalla legge*: le aziende del Gruppo, ciascuna per la propria quota parte di competenza e responsabilità, pongono in essere quanto necessario e dunque conseguente inevitabile trattamento dei dati personali (ad esempio, il provvedimento del Garante Privacy in materia di circolazione dei dati bancari [8], richiede l'approntamento e gestione dei log delle attività condotte per la banca da soggetti preposti al trattamento di dati bancari dei clienti tramite sistemi informativi, il Provvedimento del Garante Privacy relativo alla figura dell'Amministratore di Sistema [7] richiede l'approntamento e la tenuta del log dei relativi accessi ai sistemi,…);

- *individuate in conformità a quanto previsto dagli Artt. 32,34 e 35 GDPR*: le Aziende adottano necessariamente criteri di trattamento dati personali rispettando l'obbligo alla necessità e proporzionalità in osservanza dei principi ex Art. 6 GDPR nonché della prescrizione ex art 25 GDPR 'Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita', come previsto dalla Politica per la protezione dei dati personali nel Gruppo e normative interne correlate (vedasi [5]).

Trasparenza nei confronti degli Interessati

Nella Informativa ex Artt. 13 e 14 GDPR che deve essere resa ai dipendenti al momento del loro ingresso in Azienda, o successivamente nel caso intervengano aggiornamenti in merito ai loro trattamenti di dati personali,

saranno indicati specificamente e separatamente quei contesti di finalità-trattamenti per i quali l'Azienda ed i Terzi si avvalgono del Legittimo Interesse come base legale ai sensi dell'Art. 6 GDPR in relazione alla necessità di mantenere un adeguato livello di sicurezza informatica/telematica in considerazione del settore di appartenenza del Gruppo.

Pertanto, ciò comporterà:

1) in primo luogo, l'aggiornamento del Registro Attività di trattamento delle Aziende che si avvalgono del Legittimo Interesse come base legale per determinati trattamenti di dati personali dei lavoratori;
2) l'aggiornamento dell'attuale modello di Informativa per i dipendenti, che verrà utilizzato al momento dell'accensione di un nuovo rapporto 'datore di lavoro – lavoratore' all'interno del Gruppo;
3) la definizione di una strategia operativa affinché tutti coloro che sono già dipendenti di società del Gruppo, ricevano in modo documentato la Informativa aggiornata entro un prefissato periodo di tempo.

Per quanto concerne l'esercizio dei diritti dei dipendenti in qualità di Interessati, il diritto di opposizione di cui all'Art 21 GDPR è già menzionato nell'attuale modello di Informativa per i dipendenti.

Qualora l'Azienda o un Terzo (tra quelli sopra citati) riceva una richiesta di opposizione ad un trattamento basato sul Legittimo Interesse, coerentemente con quanto previsto nel comma 1 Art. 21 GDPR,

4) dovrà essere predisposta una Nota, da comunicare formalmente al richiedente, redatta sulla base di questo documento di bilanciamento di interesse e tenendo presente il caso specifico oggetto di opposizione, onde dimostrare *"l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato".*

Inoltre, laddove tali trattamenti comportino un possibile controllo remoto dei lavoratori, ciascuna Azienda del Gruppo è già vincolata, per legge ex Art. 4 Legge 300/70, a procedere, nei casi previsti dalla menzionata legge, con il preventivo Accordo Sindacale o in difetto a richiedere ed ottenere l'apposita autorizzazione da parte delle competenti autorità in materia di lavoro.
A tale proposito si evidenzia anche l'esistenza di apposita normativa interna (in relazione all'utilizzo di strumenti informatici e telematici anche in considerazione dell'apposito Provvedimento del Garante Privacy [9]) e gli accordi sindacali ex art 4 L.300/70 già in essere.

In aggiunta, laddove dall'adozione di una particolare misura possa derivare un rischio elevato per gli interessati, a titolo di esempio: adozione di misure che comportino il trattamento di dati biometrici a scopi identificativi, è attuata la valutazione ex Art. 35 GDPR, anche in considerazione delle casistiche che il Garante Privacy italiano ha individuato ai sensi del comma 4 Art. 35 GDPR.

Tempi di conservazione ed esattezza del dato

L'Azienda ed i Terzi conserveranno i dati dei dipendenti in relazione ai trattamenti qui in oggetto:

- per i tempi stabiliti per legge, laddove prescritti (vedasi ad esempio i tempi di conservazione dei log degli Amministratori di Sistema),
- tempi stabiliti da applicabili direttive da parte di Banca Italia o autorità internazionali competenti (es. European Banking Authority),

- per il tempo strettamente indispensabile di volta in volta applicabile per la specifica misura di sicurezza adottata che comporti trattamento di dati personali,
- per i tempi eventualmente derivanti da casi di accertamento, esercizio o difesa di un diritto in sede giudiziaria, dell'Azienda e di Terzi.

Per quanto concerne l'esattezza dei dati, questi sono raccolti, trattati e protetti con le dovute attenzioni, fermo restando per il singolo di potersi avvalere dell'esercizio del diritto alla rettifica di cui all'Art 16 GDPR.

Misure di sicurezza

I dati presenti nei log sono protetti da adeguate misure nel rispetto delle applicabili e specifiche previsioni di legge.

La parte riservata delle credenziali di accesso, assegnate ai singoli per poter accedere ai sistemi informativi/telematici in relazione ai loro compiti e responsabilità, è protetta in accordo a quanto specificato nelle politiche di sicurezza adottate dalle aziende del Gruppo.

Inoltre, si evidenzia che:

- la società Capogruppo è certificata ISMS (Information Security Management System) ISO/IEC 27001, e come tale adotta misure coerenti con i controlli stabiliti da tale sistema di certificazione in particolare in materia di autenticazione e misure di sicurezza relative alle credenziali di autenticazione nonché alla tenuta di log.
- I principale partner tecnologico delle aziende del Gruppo è una società anch'essa parte del Gruppo, che opera in qualità di Responsabile di trattamento dati personali ex art 28 GDPR, tenuta ad osservare le politiche di sicurezza del Gruppo ed in ogni caso ad offrire elevati standard di sicurezza in relazione ai sistemi informatici gestiti per conto delle aziende del Gruppo, anche in relazione ai processi di autenticazione e tenuta del log di loro competenza. Le misure applicate a tali sistemi sono mantenute aggiornate in funzione del progresso tecnologico ed in base alle risultanze di apposite verifiche tecniche (vulnerability assessment, penetration test, …) e di processo (verifiche periodiche in accordo a normativa specifica del settore bancario in ottica di quanto previsto dall'Art 32 GDPR). Tali verifiche sono condotte sotto la responsabilità dall'Azienda o direttamente della Capogruppo, a seconda che il sistema informativo o processo sia di gestione locale (sfera di responsabilità della singola Azienda) oppure di gruppo (sfera di responsabilità della Capogruppo).

Valutazione interessi, diritti e libertà fondamentali degli Interessati

Riguardo la possibilità che i soggetti non si aspettino ragionevolmente il trattamento in oggetto

Il personale che opera nelle Aziende del Gruppo è consapevole dell'appartenenza di queste al Gruppo e relativo settore di mercato che, anche con apposita normativa, richiede l'applicazione di elevati standard di sicurezza che non possono prescindere dall'applicazione di rigorosi processi di autorizzazione, autenticazione nonché possibilità di controllo tramite specifici log. Il personale inoltre prende parte a corsi generali in materia di privacy e, alcuni di essi, a corsi specifici in funzione delle loro mansioni (es. coloro che operano in area antiriciclaggio), nel corso dei quali è costante il riferimento a misure di sicurezza quali l'adozione di credenziali di autenticazione e la tenuta di log che comportano il conseguente trattamento dati personali riferiti ai lavoratori.

Inoltre, tutto il personale è posto a conoscenza della normativa interna di sicurezza, (es. disciplina sull'utilizzo degli strumenti informatici/telematici) e degli accordi sindacali in essere ex Art. 4 L.300/70, come previsto dalla legge applicabile.

Pertanto, non risultano elementi che possano far considerare, ad un dipendente della Azienda, inaspettato o non prevedibile un trattamento di dati a lui riferiti ai fini della sicurezza dei dati e dei processi nelle Aziende del Gruppo.

Presenza di eventuali dati connaturati da particolari caratteristiche di criticità

Tra i dati oggetto del presente trattamento possono essere presenti, nei log, informazioni relative alle azioni via via svolte da un utente di un sistema informativo, che possono comportare un controllo remoto sul lavoratore, ed in tali casi sono adottate tutte le cautele rese obbligatorie dall'Art. 4 Legge 300/70.

Impatti del trattamento sugli interessati

I trattamenti di dati del personale in forza alle Aziende del Gruppo sono volti, come già indicato, a perseguire esclusivamente finalità di sicurezza in relazione ai sistemi informativi/telematici utilizzati per la gestione delle informazioni in applicazione della normativa nazionale ed Europea nel settore bancario, per cui:

- in considerazione delle misure di sicurezza tecniche organizzative nonché delle salvaguardie che ogni Azienda del Gruppo, compresa la Capogruppo, è già tenuta a porre in essere in accordo alla Politica ICCREA [5] nel rispetto della normativa in materia di protezione dati personali, e
- tenendo presenti le salvaguardie e le ulteriori cautele indicate nelle precedenti sezioni,

i rischi derivanti sotto il profilo della riservatezza, integrità e disponibilità risultano mitigati dal complesso di tali misure, salvaguardie e cautele.

Esami di altre basi legali, alternative al Legittimo Interesse

Per i trattamenti in oggetto, non si ritiene che la relativa base legale possa essere pienamente individuata nel contratto ai sensi della lettera b comma 1 Art 6 GDPR in quanto detto contratto non intende disciplinare aspetti che dipendono dall'adozione di misure di sicurezza in relazione ai sistemi informativi impiegati nelle aziende del Gruppo.

Sono escluse per definizione le basi legali quali il Pubblico Interesse, l'Interesse vitale del singolo o di altri soggetti come anche il rispetto di una legge (lettere c), d) ed e) del comma 1 Art. 6 GDPR) in quanto non direttamente applicabili al caso in esame.

Si intende altresì escludere il ricorso al consenso lettera a) comma 1 Art. 6 GDPR in quanto:

- non si ritiene la corretta base legale per rendere lecito un trattamento che si svolge in funzione delle necessità di adottare misure di sicurezza in relazione ai sistemi informativi usati nelle aziende del Gruppo;
- l'analisi sopra documentata in relazione al bilanciamento tra gli interessi dell'Azienda e dei Terzi da una parte, e gli interessi, i diritti e le libertà fondamentali del lavoratore dall'altra, non evidenzia l'esistenza di rischi apprezzabili;
- il consenso del lavoratore, nel contesto delle finalità in oggetto non avrebbe la caratteristica di essere libero, in quanto evidentemente condizionato dai rapporti in essere tra datore di lavoro e lavoratore, come più volte

evidenziato nei lavori del WP 29 e del EDPB, ed anche dalla Decisione del Garante Privacy greco, vedasi [3] in Riferimenti.

Conclusioni

L'analisi condotta e documentata nelle precedenti sezioni, consente alla Azienda ed alle Terze Parti indicate, di avvalersi del legittimo interesse ai sensi della lettera f) comma 1 Art. 6 GDPR, non riscontrando alcuna lesione degli interessi, diritti e libertà fondamentali dei lavoratori in qualità di Interessati, fermo restando per questi la facoltà di esercitare il loro diritto di opposizione ai sensi dell'Art. 21 GDPR.

Si riepilogano qui di seguito le ulteriori cautele individuate dall'analisi, che nel loro complesso le Aziende del Gruppo, Capogruppo compresa, predispongono in relazione ai trattamenti in oggetto.

1) in primo luogo, l'aggiornamento del Registro Attività di trattamento delle Aziende che si avvalgono del Legittimo Interesse come base legale per determinati trattamenti di dati personali dei lavoratori;
2) l'aggiornamento dell'attuale modello di Informativa per i dipendenti, che verrà utilizzato al momento dell'accensione di un nuovo rapporto 'datore di lavoro – lavoratore' all'interno del Gruppo;
3) la definizione di una strategia operativa affinché tutti coloro che sono già dipendenti di società del Gruppo, ricevano in modo documentato la Informativa aggiornata entro un prefissato periodo di tempo;
4) dovrà essere predisposta una Nota, da comunicare formalmente al richiedente, redatta sulla base di questo documento di bilanciamento di interesse e tenendo presente il caso specifico oggetto di opposizione, onde dimostrare *"l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato"*.

Riferimenti

[1]	WP29 – WP 217: Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato il 9 aprile 2014
[2]	WP29 – WP 249: Parere 2/2017 sul trattamento dei dati sul posto di lavoro, adottato l'8 giugno 2017
[3]	Sintesi della decisione n. 26/2019 del Garante Privacy della Grecia, sul caso di improprio ricorso al consenso come base legale per taluni trattamenti dei dati di dipendenti da parte di PRICEWATERHOUSECOOPERS
[4]	Contratto di Coesione Gruppo
[5]	Politica per la protezione dati personali nel Gruppo e relative norme interne
[7]	**Provvedimento del Garante Privacy: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 e s.m.i.**
[8]	**Provvedimento del Garante Privacy: Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011e s.m.i.**
[9]	**Provvedimento del Garante Privacy: Lavoro: le linee guida del Garante per posta elettronica e internet - Gazzetta Ufficiale n. 58 del 10 marzo 2007 e s.m.i.**