INTRODUZIONE

La presente relazione, dopo una visione preliminare del mandato e delle funzioni di Europol ai sensi dell'*Europol Council Decision*, attuale quadro normativo di riferimento dell'UE, con particolare riguardo al regime di "*data protection*" dall'agenzia, diretta derivazione del sistema europeo di protezione dei dati di tutte le Istituzioni europee, integrato da previsioni uniche necessarie per l'assolvimento dei compiti di *intelligence* propri dell'Ufficio europeo di polizia:

- **esamina** le modalità di gestione delle informazioni di Europol;
- **individua** le Autorità nazionali ed europee preposte al controllo sul trattamento delle informazioni di Europol;
- **illustra** il quadro normativo e regolamentare dell'Unità nazionale Europol, la sua posizione ordinativa, gli organici, i compiti, la struttura e le funzioni dell'Ufficio nazionale di collegamento distaccato a L'Aia, i flussi informativi da e verso Europol e le comunicazioni con le Autorità nazionali competenti, secondo i vigenti criteri di competenza per materia o di maggior concentrazione delle informazioni investigative.

Si esaminano quindi i carichi di lavoro dell'UNE e i volumi complessivi di corrispondenza operativa inclusivi di un prospetto allegato con le principali operazioni di polizia portate a termine dalle Forze di polizia nazionali attraverso il canale della cooperazione internazionale Europol.

Vengono quindi svolte brevi considerazioni riguardanti lo stato del dibattito preliminare all'emanazione del nuovo Regolamento di Europol che entrerà in vigore nel 2014 e che, per caratteristica dello strumento normativo, a portata generale, obbligatorio in tutti i suoi elementi e direttamente applicabile, imporrà - realisticamente - passi obbligatori agli Stati membri ed ancora sulla presenza degli italiani nello *staff* di Europol e sui costi dell'organizzazione per i servizi erogati a favore dei Paesi dell'UE.

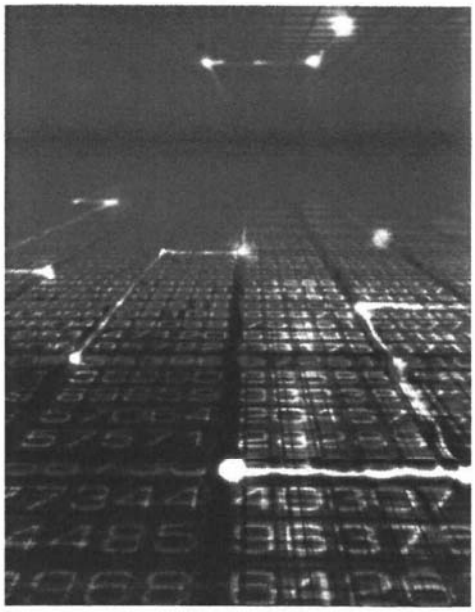
1. Il mandato di Europol.

Il mandato di Europol è definito dall'art. 4 comma 1 della Decisione istitutiva del 2009. Le sue competenze coprono il terrorismo e la criminalità organizzata così come le altre forme gravi di criminalità (c.d."*serious crime*") come elencate nell'annesso alla richiamata Decisione, quali ad esempio il traffico di esseri umani, la contraffazione degli Euro o i crimini collegati agli stupefacenti. E' tuttavia necessario che i crimini riguardino due o più Stati membri perché si possa richiedere un'azione comune.

Anche il tipo di azione che Europol può intraprendere è chiaramente definito nella Decisione. Europol è un'agenzia europea il cui principale obiettivo è di supportare ed assistere gli Stati membri nei loro sforzi per prevenire e combattere il crimine organizzato, il terrorismo e le altre forme gravi di criminalità ("*serious crime*", citati) (art. 3 Decisione).

Ai sensi dell'art. 5 della Decisione i compiti principali sono:
- raccogliere, collazionare ed analizzare informazioni e *intelligence*;
- agevolare lo scambio d'informazioni tra Stati membri;
- assistere le investigazioni nazionali;
- aiutare nel coordinamento di operazioni collettive;
- preparare valutazioni delle minacce, analisi strategiche e rapporti generali di situazione;
- condividere *expertise* e conoscenze.

2. Il regime di protezione dei dati di Europol.



La legislazione per la protezione dei dati ad Europol

- Decisione del Consiglio Europol
- Regole di attuazione (es. Regole sugli AWFs, Regole per le relazioni con le Parti terze, Regole sulla protezione del segreto delle informazioni di Europol)
- Regolamento CE 45/2001
- Convenzione 108 del Consiglio (1981)
- Raccomandazioni del Consiglio R (87) 15

Riconoscendo l'importanza di una chiara legislazione nell'area della protezione dei dati, l'Unione Europea ha creato una forte cornice legale di riferimento realizzata a misura per salvaguardare i diritti fondamentali dei suoi cittadini. All'interno di questa cornice lo strumento di riferimento è la Direttiva 95/46/EC[1] che individua regole essenziali per il trattamento e il movimento dei dati personali.
Se, da un lato, la necessità di salvaguardare i dati gestiti per le finalità di Europol è indiscutibile, dall'altro, non vi è dubbio che i compiti dell'agenzia richiedano un lavoro di "*intelligence*" di livello elevato.
I cambiamenti legislativi in quest'area hanno avuto pertanto lo scopo d'individuare un punto di equilibrio tra gli interessi fondamentali di libertà e quelli di sicurezza.
Nel caso di Europol fu chiaro sin dall'inizio che doveva essere creato un quadro di regole che potevano tenere in conto tanto le esigenze operative di Europol quanto i diritti individuali e l'effettiva protezione dei dati.

In risposta a questi cambiamenti fu realizzata una legislazione specializzata e, pertanto, Europol dispone (nell'autopercezione dell'agenzia) di una delle più forti e robuste cornici di protezione dei dati nel mondo delle forze di polizia. La pietra angolare per raggiungere il tipo di bilanciamento immaginato è stata proprio la Decisione istitutiva (d'ora in avanti *Europol Council Decision* - ECD). Con questa Decisione, gli Stati membri riconobbero la necessità di prevedere regole speciali, fatte appositamente per la protezione dei dati di Europol. Per evidenziare l'esigenza, il legislatore specificò che la previsione della protezione dei dati personali era essenziale per la particolare natura, funzione e competenza di Europol. Conseguentemente la Decisione riflette gli stessi valori della Direttiva 95/46/EC ma contiene anche previsioni dettagliate e uniche per Europol.
La Decisione è ulteriormente integrata da un panorama di regole di attuazione, in particolare le regole che riguardano gli AWFs, che disciplinano la gestione dei file di lavoro per fini di analisi di Europol.

[1] Dir. 24 ottobre 1995, n. 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

L'Agenzia, inoltre, osserva i principi del Regolamento 45/2001[2] con riguardo al trattamento dei dati dello *staff*.
Lo standard di protezione dei dati di Europol come definito nell'art. 27 dell'ECD, si riallaccia ai principi della Convenzione del Consiglio d'Europa 108[3] e alla raccomandazione n. R (87) 15[4].

Una delle principali implicazioni di questo sofisticato regime di protezione dei dati di Europol è che le informazioni di Europol possono essere trattate solo se ciò è permesso dalla legge e, per assicurare che ciò avvenga, le regole che governano il trattamento dei dati devono essere inequivoche e definitive. Il presupposto per il raggiungimento è l'adozione di una chiara terminologia cosicché i termini utilizzati nell'ECD e nelle ulteriori regole di attuazione fanno uso di terminologie comuni al mondo della protezione dei dati come "dati personali" e "trattamento dei dati".

In termini pratici il trattamento dei dati ad Europol avviene con l'aiuto di *software* appositamente realizzati.

---

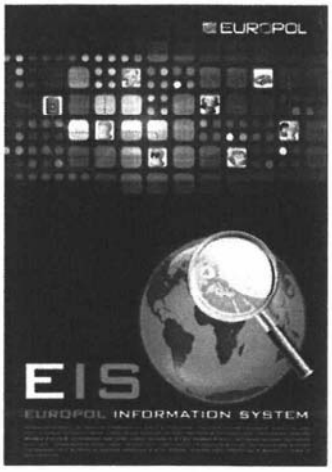
[2] Reg. (CE) 18 Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.

[3] Convenzione per la protezione degli individui con riguardo al trattamento automatico dei dati personali, aperto per la firma a Strasburgo il 28 gennaio 1981.

[4] Del Comitato dei Ministri agli Stati Membri per la regolamentazione dell'uso dei dati personali nel settore di polizia, adottata il 17 settembre 1987.

3. Il sistema d'informazione di Europol - Europol information system (EIS).

Uno dei *database* centrali di Europol è l'*Europol Information System* (EIS). Attraverso questo sistema gli Stati membri possono condividere e ricercare informazioni sul conto di persone, eventi e dispositivi connessi a vicende criminali (es. sospetti, armi, telefoni, numeri di telefono, numeri di targa, passaporti).



La gamma di dati che può essere processata è comunque limitata: soli i dati che sono necessari per le funzioni di Europol possono essere utilizzati (art. 12, comma 1 ECD). I dati in EIS devono essere correlati a sospetti, criminali colpevoli o persone per le quali vi siano indizi concreti o ragionevoli motivi per ritenere che possano commettere crimini che rientrano nel mandato di Europol. L'art. 12 comma 2 dell'ECD contiene una lista esaustiva del tipo di dati (c.d. oggetti) che possono essere conservati e trattati: nomi, date e luoghi di nascita, nazionalità, sesso, luoghi di residenza, professione, documenti d'identità, impronte digitali e profili di DNA. Grazie agli sviluppi tecnologici, i dati non devono essere inseriti manualmente nell'EIS. *Dataloader* appositamente designati sono stati installati in molti *database* nazionali per caricare automaticamente quantità rilevanti di dati. Organizzazione e misure di sicurezza tecnologiche assicurano che solo i dati che riguardano il mandato di Europol vengano trasmessi. Questo caricamento selettivo viene indicato da Europol come esempio di *"privacy by design"*, fin dalla progettazione finalizzata a garantire un alto livello di protezione dei dati in uso ad Europol.
L'ammontare dei dati caricati per mezzo di *dataloaders* viene inoltre definito dall'agenzia come ragguardevole essendone reperibili nel sistema circa 200.000 e risultando eseguite, approssimativamente, 10.000 ricerche con riscontri positivi ogni mese.

I dati trattati in EIS non possono essere conservati indefinitamente: Europol può custodirli per un ben definito periodo di tempo (art. 20 ECD). In generale le informazioni possono essere trattenute solo per il tempo necessario e debbono essere revisionate non più tardi di tre anni dal loro inserimento.
La revisione deve comunque avere luogo nel caso in cui sorgano circostanze che richiedono l'eliminazione dei dati. Per esempio, i dati in EIS devono essere cancellati quando le persone sono state assolte o quando i procedimenti contro di loro sono stati definitivamente archiviati (art. 12 comma 5, ECD).

4. I file di lavoro per fini di analisi - Analysis Work Files (AWFs).

L'analisi criminale per il supporto alle operazioni ad Europol s'identifica con i *file* di lavoro per fini di analisi (Analysis Work Files - AWFs) che vengono definiti come cornice della cooperazione operativa nell'UE. Al contrario di EIS, gli AWFs sono *database* focalizzati sull'analisi criminale in una specifica area. Fenomeni dedicati possono essere traguardati individualmente e raggruppati allo scopo di fermarli (es. terrorismo islamico, traffico di esseri umani, riciclaggio, ecc.) permettendo la raccolta e l'analisi di dati rilevanti in un ambiente unico.

Conformemente, i dati degli AWFs, possono non solo essere connessi a sospetti (futuri) criminali ma anche a contatti, soci, testimoni, vittime, informatori. La lista delle categorie di dati (ai sensi dell'art. 6 delle c.d. AWF Rules[5]) che possono essere conservati è più ampia di quella di EIS. Tuttavia, regole supplementari di protezione dei dati vengono applicate e garantiscono l'impiego responsabile delle informazioni contenute in questo ambiente.

L'accesso agli AWFs e al contenuto dei *file* individuali è strettamente limitato dai loro rispettivi Ordini di apertura (art. 5 delle AWFs Rules). In via preliminare, l'Ordine di apertura, specifica lo scopo del *file*. Le informazioni che non riguardano la descrizione dello scopo non possono essere inserite in un AWF. I dati contenuti negli AWF, inoltre, non possono essere utilizzati per altre ragioni quali, ad esempio, addestramento o inchieste amministrative. L'art. 4 delle AWF *Rules*, inoltre, stabilisce che i dati personali possono essere trattati solo nella misura in cui essi siano adeguati, accurati, pertinenti e non vadano oltre lo scopo dell'archivio di lavoro per fini di analisi nel quale sono introdotti e a condizione che siano conservati solo per il tempo necessario a detto scopo.

Inoltre, l'art. 14 comma 1 della Decisione, enfatizza che i dati sensibili personali possono solo essere trattati dove strettamente necessario per i propositi del *file*.

Ancora, gli Ordini di apertura determinano la natura dei dati e degli individui sui quali i dati possono essere conservati, le condizioni sotto le quali possono essere comunicati a certi destinatari e le procedure appropriate per fare ciò, così come i limiti di custodia delle informazioni medesime. Con riguardo alla custodia dei dati i principi sono i medesimi applicati per EIS (art. 20 comma 1, ECD).

---

[5] Decisione 30 novembre 2009, n. 2009/936/GAI che adotta le norme di attuazione degli archivi di lavoro per fini di analisi di Europol.

La partecipazione alle attività di analisi è limitata espressamente al c.d. *Gruppo di analisi*: in generale si tratta di elementi designati dello *staff* di Europol sebbene Ufficiali di collegamento e/o esperti degli Stati membri possano unirsi a un particolare *file*. Si possono anche associare le c.d. Parti terze alle attività dei gruppi di analisi e ricevere i risultati che li riguardano.
Allo stesso tempo, i membri dei gruppi di analisi possono porre limiti all'uso dei loro dati assegnando predefiniti codici di maneggio (c.d. *handling code*). Per esempio si possono determinare o escludere potenziali destinatari (art. 14 comma 6 ECD).

Per permettere agli AWFs di funzionare e consentire analisi efficienti, i dati nei *file* devono essere interamente verificati: solo l'alta qualità delle informazioni, nel pensiero di Europol, genera alta qualità delle analisi. Le Autorità delle Forze di polizia devono pertanto vagliare le informazioni fornite da Europol per verificare che siano corrette e valide. Come risultato, Europol può solo trattare dati se accurati ed aggiornati. Dopo un iniziale controllo all'immissione dei dati, verifiche regolari devono essere svolte per assicurare che i dati continuino a raggiungere i requisiti richiesti (artt. 27 e 29 comma 1 dell'ECD e 5 della Convenzione 108). *Auditing* regolari sono necessari e vengono periodicamente eseguiti per assicurare il buon funzionamento degli AWFs.

5. Sicurezza delle informazioni.

Un altro importante aspetto in connessione con i *database* di Europol è la sicurezza delle informazioni. Le misure di sicurezza sono reputate essenziali non appena dati personali o sensibili strategici vengono trattati. Sotto il regime dell'ECD Europol ha l'obbligo di accrescere le tecnologie e le misure organizzative necessarie per proteggere i suoi dati (art. 35 ECD). Conseguentemente sono stati realizzati alcuni dispositivi tecnologici ad Europol per prevenire l'accesso o l'uso non autorizzato dei dati. Sono altresì garantite protezioni concrete contro la perdita di dati o il malfunzionamento dei sistemi.

L'accesso alle informazioni e il loro maneggio è definito e ristretto da una classificazione applicabile. L'agenzia individua tre tipi di informazioni Europol:

- *Europol public information*;
- *Europol Unclassified - Basic Protection Level Information;*
- *Europol classified information.*

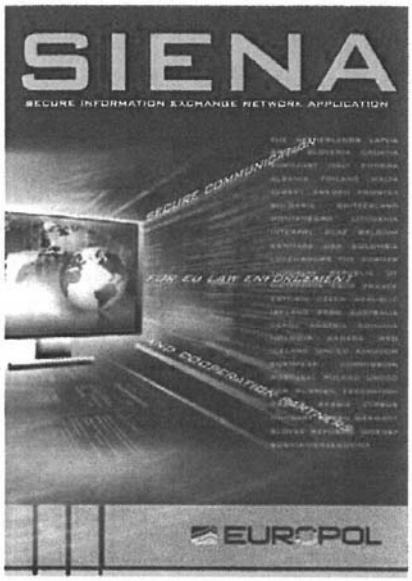
Le *Europol classified information* sono ulteriormente suddivise in quattro sottocategorie a seconda del potenziale impatto che potrebbe essere causato da un accesso non autorizzato:

- *EU RESTRICTED;*
- *EU CONFIDENTIAL;*
- *EU SECRET;*
- *EU TOP SECRET.*

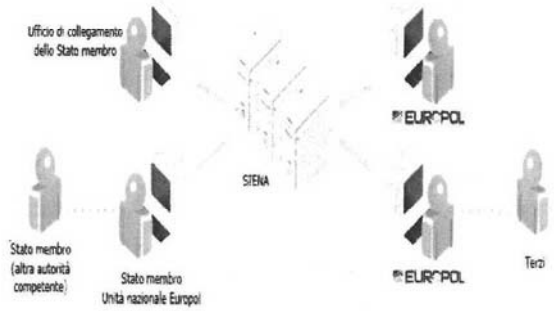
A ciascun tipo d'informazioni si affianca un *set* di misure di sicurezza che deve essere applicato per proteggerle contro gli accessi non autorizzati. Per esempio, le informazioni catalogate come *EU Confidential* o superiori possono solo essere create o riprodotte attraverso ufficiali appositamente autorizzati utilizzando speciali e sicuri equipaggiamenti in modo da assicurare la piena tracciabilità dei testi scritti.

6. SIENA - Secure Information Exchange Network Application.

Dopo la presentazione del principale sistema di Europol per il trattamento dei dati e il suo approccio generale verso la sicurezza delle informazioni occorre chiarire come queste informazioni prendano la loro via nel sistema Europol.



Poiché l'agenzia è essenzialmente concentrata sullo scambio d'informazioni, la sicurezza e la velocità di trasmissione dei dati di pertinenza è ritenuta essenziale. Le informazioni da uno Stato membro devono poter raggiungere Europol senza rischi d'intercettazione e vice versa. Al fine di scambiare informazioni velocemente e in sicurezza, è stato progettato da Europol un sistema *ad hoc* denominato *Secure Information Exchange Network Application* – SIENA.

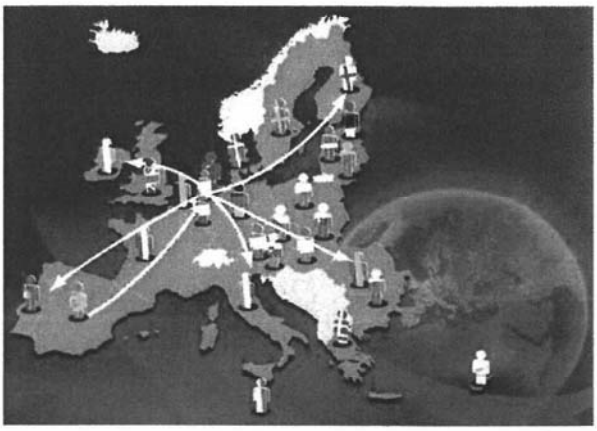


Così come avviene per la custodia e l'analisi dei dati, la trasmissione dei dati da e verso Europol deve avvenire nel rispetto dei principi di protezione dei dati e della salvaguardia della sicurezza delle informazioni. La piattaforma informatica SIENA, ospitata in un ambiente sicuro del nuovo Quartier Generale di Europol, permette agli Stati membri, alle parti terze e ad Europol di comunicare velocemente e in modo sicuro attraverso un canale di comunicazione di agevole uso.
Europol è obbligata a tenere registrazioni della trasmissione dei dati. In forza di tale esigenza, il SIENA documenta automaticamente tutti i processi di comunicazione. Per garantire ulteriormente il maneggio

responsabile dei dati personali, l'informazione è trasmessa da Europol ad altri *partners* solo se il ricevente dà assicurazione che i dati saranno usati per gli scopi per i quali sono stati trasmessi (art. 24 comma 2 ECD).

7. Gli uffici nazionali di collegamento presso Europol (Liaison Bureau).

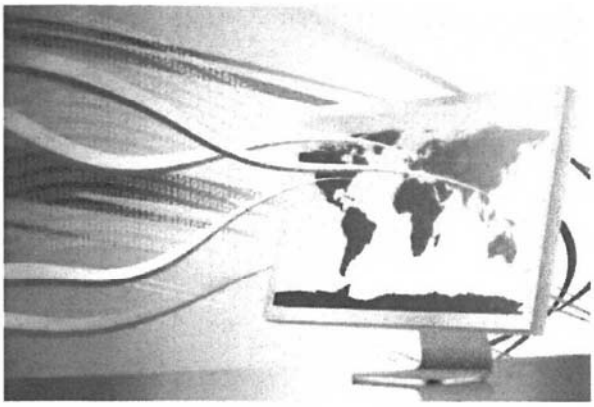
Le previsioni tecniche per l'ottimizzazione dello scambio d'informazioni ruotano attorno al concetto unico dell'Europol Liaison Bureau. Ciascuno Stato membro invia almeno un rappresentante al Quartier Generale di Europol che, a sua volta, garantisce a ciascuno Stato membro la disponibilità dei locali necessari (art. 9 ECD). Inoltre, gli Stati terzi che hanno concluso con Europol un accordo di cooperazione sono rappresentati da almeno un Ufficiale di collegamento, come accade per INTERPOL. Complessivamente Ufficiali di collegamento di 36 Paesi più INTERPOL sono collocati in un'area di Europol, rendendo le comunicazioni tra loro e le loro rispettive autorità nazionali facili e veloci.



Gli Ufficiali di collegamento sono presenti e/o reperibili 24 ore al giorno, sette giorni su sette, in contatto con le loro Unità nazionali designate (art. 8 ECD) via SIENA. Gli agenti delle forze di polizia dei Paesi partecipanti indirizzano richieste e messaggi all'Unità Nazionale che li invia agli Uffici di collegamento. In questo modo, le barriere di linguaggio sono effettivamente superate: gli Ufficiali di collegamento possono comunicare con le UNE nella loro lingua madre ricevendo una risposta nella stessa lingua.
Questa capacità di traduzione unita alla prossimità degli uffici sono considerati da Europol come risorse dai risvolti estremamente positivi per l'esecuzione di ogni operazione transfrontaliera.

L'Italia, in questo momento, distacca dall'UNE cinque Ufficiali di collegamento presso il proprio LB (tre funzionari, rispettivamente della P di S, dei CC e della G di F, più due Ispettori della P di S).

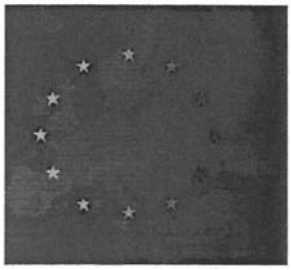
8. L'acquisizione d'informazioni extra Europol.



Le regole di protezione dei dati sono applicate a tutte le forme di scambio di dati personali tra Europol e gli Stati membri. Tuttavia, la rete d'informazioni di Europol si estende oltre i Paesi dell'UE. Riconoscendo come le informazioni delle parti terze possano essere in molti casi benefiche, Europol mantiene numerosi contatti esterni ed accordi di cooperazione. Per ciascun sistema di comunicazione di dati con entità esterne sono state realizzate nell'ECD regole forti per garantire che i suoi *standard* siano applicati anche in questi casi. Per esempio, i dati non possono essere trasmessi ad entità terze senza il preventivo consenso del legittimo proprietario (art 24. comma 1 ECD).
Poiché le parti terze non sono soggette al regime di protezione dei dati dell'ECD, Europol deve assicurare che sia comunque attuato un adeguato livello di tutela delle informazioni; tanto con riferimento alla protezione dei diritti e delle libertà fondamentali dei soggetti cui le informazioni si riferiscono quanto con riguardo al trattamento di tali dati, così come ai rischi in tema di sicurezza nel trasferimento di informazioni classificate.

Acquisizione d'informazioni da:

a. **Istituzioni dell'UE.**



Per quanto riguarda lo scambio di dati tra istituzioni europee, l'art. 22 dell'ECD prevede una base per Europol per stabilire e mantenere relazioni di cooperazione con una serie di istituzioni ed agenzie europee, come Eurojust, la BCE o l'Ufficio europeo antifrode (OLAF). Dove accordi non sono ancora stati conclusi, Europol può ancora scambiare informazioni, inclusi dati personali, attestando che lo scambio è necessario per i compiti dei destinatari.