CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 28 febbraio 2014 (OR. en)

6762/1/14 REV 1

Fascicolo interistituzionale: 2012/0011 (COD)

DATAPROTECT 30
JAI 102
MI 191
DRS 26
DAPIX 25
FREMP 28
COMIX 110
CODEC 503

NOTA

della:	presidenza
al:	Consiglio
n. doc. prec.:	17831/13 DATAPROTECT 201 JAI 1149 MI 1166 DRS 223 DAPIX 158 FREMP 209 COMIX 700 CODEC 2973 5879/14 DATAPROTECT 13 JAI 46 MI 91 DRS 14 DAPIX 7 FREMP 12 COMIX 68 CODEC 230 5881/14 DATAPROTECT 15 JAI 48 MI 93 DRS 16 DAPIX 9 FREMP 14 COMIX 70 CODEC 232 5344/1/14 REV 1 DATAPROTECT 4 JAI 22 MI 38 DRS 7 DAPIX 4 FREMP 4 COMIX 28 CODEC 91
Oggetto:	Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) [prima lettura] Dibattito orientativo su talune questioni

I. Introduzione

1. Il Consiglio tratta il pacchetto sulla protezione dei dati, presentato dalla Commissione il 25 gennaio 2012, come una priorità chiave. Il pacchetto sulla protezione dei dati comprende due proposte legislative basate sull'articolo 16 del TFUE. La prima proposta, relativa a un regolamento generale sulla protezione dei dati, è intesa a sostituire la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. La seconda proposta, relativa a una direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, e la libera circolazione di tali dati, è intesa a sostituire la decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

2. Il Consiglio europeo del 24 e 25 ottobre 2013, che si è concentrato sull'economia digitale, l'innovazione e i servizi, ha concluso che "l'adozione tempestiva di un solido quadro generale dell'UE per la protezione dei dati e della direttiva sulla sicurezza informatica è essenziale per il completamento del mercato unico digitale entro il 2015."

3. Nei primi due mesi del suo mandato, la presidenza ha proceduto, sulla scorta dei lavori svolti dalle presidenze danese, cipriota, irlandese e lituana, ad approfondite discussioni su taluni aspetti importanti della riforma. La presidenza ha dedicato più di 10 riunioni di un'intera giornata al pacchetto legislativo sulla protezione dei dati (regolamento e direttiva).

4. Nelle discussioni informali tenute ad Atene il 23 e 24 gennaio 2014, i ministri della giustizia si sono detti complessivamente soddisfatti delle disposizioni del progetto di regolamento per quanto riguarda le questioni internazionali e hanno incoraggiato l'eventuale rafforzamento di tali modelli con altri modelli alternativi. Nel mondo globalizzato di oggi, tali disposizioni sono essenziali per assicurare la continuità dell'elevato livello di protezione offerto ai cittadini dell'UE quando sono presi di mira da imprese stabilite al di fuori dell'UE e in caso di trasferimento dei loro dati personali verso paesi terzi o organizzazioni internazionali.

5. Il regolamento generale sulla protezione dei dati si fonda sul sistema e i principi comprovati della direttiva sulla protezione dei dati (direttiva 95/46/CE). Nel quadro della procedura di comitato e con la partecipazione dei rappresentanti degli Stati membri e del Parlamento europeo, la Commissione può decidere se il livello di protezione assicurato da un paese terzo – inclusi taluni territori o settori di trattamento - o da un'organizzazione internazionale sia adeguato. Il comitato europeo per la protezione dei dati sarà consultato ed esprimerà il suo parere. Una delle decisioni di adeguatezza adottate dalla Commissione riguarda i trasferimenti di dati a fini commerciali tra l'UE e gli USA (decisione 2000/520/CE della Commissione), la cosiddetta decisione "approdo sicuro". Lo scorso novembre la Commissione ha presentato la comunicazione "Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA" e attualmente conduce intense discussioni con le controparti statunitensi sul regime "Approdo sicuro" al fine di rafforzarlo entro l'estate.

6. Il progetto di regolamento prevede inoltre che i trasferimenti verso i paesi terzi possano aver luogo se il responsabile del trattamento o l'incaricato del trattamento applica garanzie adeguate, incluse norme vincolanti d'impresa e clausole contrattuali. Il ruolo dei codici di condotta approvati e dei meccanismi di certificazione approvati è stato rafforzato. Tali trasferimenti dovrebbero aver luogo su un piano di parità con quelli basati sulle decisioni di adeguatezza. In situazioni particolari, i trasferimenti possono anche essere basati su deroghe limitate.

7. Sulla scorta dei risultati del Consiglio di giugno 2013, il Gruppo "Scambio di informazioni e protezione dei dati" (DAPIX) ha effettuato un ulteriore esame di aspetti specifici dei capi da I a IV. Discussioni approfondite si sono svolte sul diritto alla portabilità dei dati e sulla profilazione nonché sulla pseudonimizzazione e sugli obblighi del responsabile del trattamento e dell'incaricato del trattamento. In seguito a tali discussioni, la presidenza si è impegnata a riformulare ulteriormente punti specifici dei capi da I a IV.

8. La presidenza acclude il testo sul campo di applicazione territoriale, sul capo V (Trasferimenti internazionali) e su importanti punti specifici dei citati capi da I a IV (...). Il testo che figura negli allegati I e II rispecchia i risultati delle discussioni svoltesi durante le presidenze danese, cipriota, irlandese, lituana e greca.

9. Durante la presidenza greca si sono compiuti ulteriori progressi sostanziali nel negoziato del progetto di regolamento. Sono in corso discussioni sul meccanismo di sportello unico sulla base delle indicazioni fornite dai ministri nei Consigli GAI di ottobre e dicembre 2013.

II. Campo di applicazione territoriale e principi fondamentali dei trasferimenti internazionali

10. Nelle discussioni informali di Atene del gennaio 2014, i ministri si sono detti complessivamente soddisfatti delle disposizioni del progetto di regolamento sulle questioni internazionali e del campo di applicazione territoriale del regolamento, rilevando la necessità di assicurare in generale l'applicazione delle norme dell'Unione ai responsabili del trattamento che non sono stabiliti nell'UE quando trattano i dati personali dei residenti dell'Unione.

    I ministri hanno inoltre sottolineato il carattere eccezionale della trasmissione di dati personali verso paesi terzi o organizzazioni internazionali basata su deroghe (e non, cioè, su accertamenti di adeguatezza/garanzie adeguate, incluse le norme vincolanti d'impresa o le clausole contrattuali) e la necessità di fornire salvaguardie intese a garantire i diritti e le libertà fondamentali per quanto riguarda la protezione dei dati personali sanciti dall'articolo 8 della Carta dell'UE.

    Riguardo ad eventuali nuovi modelli futuri (alternativi) che potrebbero essere presi in considerazione per i trasferimenti internazionali, la presidenza ritiene che essi possano e debbano iscriversi nella logica del sistema - multiforme ma coerente - attualmente proposto che muove da trasferimenti basati su accertamenti di adeguatezza, garanzie adeguate e deroghe, cui i ministri hanno dato il loro sostegno durante le discussioni informali tenutesi ad Atene. L'attuale compromesso è adeguato alle esigenze future e offre sufficienti possibilità di soddisfare nuovi modelli basati su garanzie adeguate che assicurino la tutela delle persone fisiche i cui dati sono trasferiti all'estero.

III. Disposizioni fondamentali - Capi da I a IV

I quattro temi da discutere riguardano alcuni sviluppi tecnologici chiave degli ultimi anni. In ciascun caso, la presidenza mira a garantire che venga sviluppato appieno il potenziale del regolamento proposto in modo da accrescere la fiducia nel mercato unico digitale dell'UE.

Pseudonimizzazione

11. La pseudonimizzazione dei dati personali è un'operazione comune nel mondo digitale e uno dei mezzi più importanti per garantire la protezione dei dati nell'ambito di un approccio fondato sul rischio. Per tale motivo la pseudonimizzazione dovrebbe essere incoraggiata laddove tali dati continuano ad essere dati personali. Il dibattito a livello tecnico ha portato all'inserimento della "pseudonimizzazione" nel regolamento al fine di limitare l'impatto sui diritti individuali e rafforzare la sicurezza dei dati. Contribuirà a stabilire il giusto equilibrio tra la tutela dei diritti e delle libertà fondamentali delle persone fisiche interessate e l'esigenza del settore pubblico e privato di trattare grandi quantità di dati. Un esempio di pseudonimizzazione potrebbe essere rappresentato dal caso in cui i dati medici di pazienti malati di cancro siano sottoposti ad un processo di eliminazione degli elementi identificativi diretti, quali il nome, e di attribuzione casuale di numeri di serie a ciascun paziente, in modo che le informazioni così ottenute possano essere utilizzate a fini di ricerca medica o di salute pubblica.

Portabilità dei dati personali

12. Il diritto alla portabilità dei dati mira a permettere alle persone fisiche di trasferire i loro dati personali da un prestatore all'altro quando decidono di optare per un altro prestatore (ad es., trasmissione dei dati di una persona fisica relativi alla sua esperienza professionale da una rete sociale a finalità generale ad una rete orientata alla carriera professionale). Le discussioni hanno mostrato l'importanza che il diritto alla portabilità dei dati riveste per consentire alle persone fisiche di avere il controllo sui loro dati, specie su Internet, e per modernizzare il quadro attuale. La presidenza è venuta incontro alle preoccupazioni espresse da alcune delegazioni eliminando il settore pubblico dal campo di applicazione del diritto alla portabilità dei dati e migliorandone la portata per evitare eccessivi oneri ai responsabili del trattamento dei dati. Il compromesso assicura la tutela di altre persone fisiche interessate e tiene conto dell'esigenza di neutralità tecnologica.

Obblighi dei responsabili del trattamento e degli incaricati del trattamento

13. Oggi i prestatori di servizi svolgono nell'economia digitale un ruolo di gran lunga più importante che nel 1995. I nuovi sviluppi tecnologici, segnatamente nel cloud computing, richiedono di migliorare e precisare il ruolo e gli obblighi dei responsabili del trattamento e degli incaricati del trattamento (inclusi i sub-incaricati) nel trattamento dei dati. La presidenza ha cercato di chiarire il rapporto tra i responsabili del trattamento e gli incaricati del trattamento, anche attraverso l'inclusione di un riferimento a contratti facoltativi "standardizzati" tra i responsabili del trattamento e gli incaricati del trattamento. Le discussioni a livello tecnico hanno mostrato l'esistenza di un sostegno in proposito.

Automazione della decisione basata sulla profilazione

13. Il trattamento dei dati personali è assolutamente essenziale per un'economia basata sulla conoscenza. Nell'era digitale molte attività economiche si basano sulla creazione e utilizzazione di taluni profili. Perciò la pubblicità via Internet, che rappresenta in se stessa un importante fondamento economico di Internet, è spesso basata sulla creazione e l'utilizzazione di taluni profili per finalità di marketing. La creazione e l'utilizzazione di profili degli utenti può essere anche impiegata per tutelare questi ultimi, ad es. da frodi legate alle carte di credito o da altri tipi di frode in un ambiente digitale.

Tuttavia, il trattamento inteso a valutare (ossia, analizzare e prevedere) taluni aspetti relativi al rendimento professionale, alla situazione economica, allo stato di salute, alle preferenze personali o agli interessi, all'affidabilità o al comportamento, all'ubicazione o agli spostamenti (profilazione) possono comportare gravi rischi per i diritti e le libertà delle persone fisiche. In virtù della direttiva del 1995 (articolo 15), già esiste una disposizione sul diritto di una persona di non essere sottoposta ad una decisione fondata esclusivamente su un trattamento automatizzato e che produca effetti giuridici o abbia effetti significativi nei suoi confronti in considerazione di alcuni dei suddetti aspetti. La decisione in questione potrebbe contemplare attività quali il rifiuto automatizzato di una domanda di credito online senza alcun intervento umano. Pertanto, tale disposizione mira soprattutto a evitare che le persone fisiche siano sottoposte ad una automazione della decisione senza l'intervento umano.

L'attuale compromesso non introduce un regime specifico che disciplina le attività di profilazione in quanto tali. Esso assoggetta tali attività alle norme generali che disciplinano il trattamento dei dati personali (basi giuridiche del trattamento, principi di protezione dei dati) con specifiche garanzie (ad esempio, obbligo di effettuare una valutazione d'impatto in alcuni casi (articoli 33 e 34) o disposizioni relative alle informazioni specifiche da fornire alla persona fisica interessata. Il comitato europeo per la protezione dei dati avrebbe la possibilità di emanare orientamenti in tale contesto.

La presidenza intende garantire che la persona fisica venga tutelata contro decisioni assunte esclusivamente sulla base di un trattamento automatizzato, inclusa la profilazione, che producano effetti giuridici che lo riguardano o incidano gravemente sulla sua persona.

Il testo attuale cerca di vietare la decisione basata sul trattamento automatizzato, segnatamente (ma non esclusivamente) attraverso la profilazione, ma non la creazione e l'utilizzazione di profili in quanto tali.

L'automazione della decisione dovrebbe essere consentita solo se necessaria per la conclusione o l'esecuzione di un contratto, sulla base di un esplicito consenso dell'interessato o qualora esplicitamente autorizzata dal diritto dell'Unione o di uno Stato membro, incluso per la prevenzione delle frodi e dell'evasione fiscale e a fini di monitoraggio.

La profilazione e l'automazione della decisione basate su categorie particolari di dati personali dovrebbero essere consentite solo a determinate condizioni.

IV. Quesiti

La presidenza è consapevole che il sostegno accordato a qualsiasi questione è condizionato, nel senso che nessuna parte del progetto di regolamento può essere approvata in via definitiva finché non è approvato l'intero testo del regolamento.

Alla luce di ciò si invita il Consiglio a:

A. *esaminare se in seguito alle discussioni della riunione informale dei ministri tenutasi ad Atene, conferma il suo ampio sostegno ai progetti di disposizioni per quanto riguarda il campo di applicazione territoriale del regolamento (articolo 3, paragrafo 2) (cfr. allegato I);*

B. *esaminare se, in seguito alle discussioni del Consiglio informale di Atene, conferma il suo avallo ai principi fondamentali del Capo V (allegato II) quale base per il completamento delle discussioni tecniche sul tale capo in sede di gruppo "Scambio di informazioni e protezione dei dati" (DAPIX);*

C. *confermare che il gruppo "Scambio di informazioni e protezione dei dati" (DAPIX) dovrebbe proseguire i lavori sulla base dei progressi compiuti sinora e completare i lavori riguardanti:*
   1) *la pseudonimizzazione in quanto elemento dell'approccio fondato sul rischio* (ved. allegato III);
   2) *la portabilità dei dati personali per il settore privato (ved. allegato IV);*
   3) *gli obblighi dei responsabili del trattamento e degli incaricati del trattamento (ved. allegato V).*

D. *esaminare se il progetto di regolamento, al pari della direttiva 95/46/CE debba*
   a. *limitarsi a disciplinare l'automazione della decisione segnatamente (ma non esclusivamente) basata su profili che ha effetti giuridici o incide significativamente sulle persone fisiche; o*
   b. *debba prevedere anche un regime specifico riguardo alla creazione e all'utilizzazione di profili.*

_____

CAMPO DI APPLICAZIONE TERRITORIALE

19) Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o incaricato del trattamento nel territorio dell'Unione deve essere conforme al presente regolamento, che il trattamento avvenga all'interno dell'Unione o al di fuori. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica.

20) Onde evitare che una persona fisica venga privata della tutela cui ha diritto in base al presente regolamento, è necessario che questo disciplini anche il trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono legate all'offerta di beni o servizi a dette persone indipendentemente dal fatto che vi sia un pagamento o no,**(...)all'interno dell'Unione**. Per determinare se tale responsabile del trattamento stia offrendo beni o servizi a dette persone nell'Unione, occorre verificare se risulta che il responsabile del trattamento intenda concludere affari con residenti in uno o più Stati membri dell'Unione. Se la semplice accessibilità del sito Internet del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica, di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il responsabile del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, e/o la menzione di clienti o utenti residenti nell'Unione, possono evidenziare l'intenzione del responsabile del trattamento volta all'offerta di beni o servizi a dette persone nell'Unione **(...)**.

21) È opportuno che anche il trattamento dei dati personali di residenti nell'Unione ad opera di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al controllo del loro comportamento all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al "controllo del comportamento" dell'interessato, occorre verificare se le operazioni che questi esegue su Internet sono sottoposte a tecniche di trattamento dei dati volte alla profilazione dell'utente, in particolare per prendere decisioni che li riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.

22) Laddove vige la legislazione nazionale di uno Stato membro in virtù del diritto internazionale pubblico, ad esempio nella rappresentanza diplomatica o consolare di uno Stato membro, il presente regolamento deve applicarsi anche a un responsabile del trattamento non stabilito nell'Unione

Articolo 3 *Campo di applicazione territoriale*

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione.

2. Il presente regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
   a) l'offerta di beni o la prestazione di servizi ai suddetti residenti nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
   b) il controllo del loro comportamento, quest'ultimo inteso all'interno dell'Unione europea.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un responsabile del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto nazionale di uno Stato membro in virtù del diritto internazionale pubblico.

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to **recipients in** third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to **recipients in** another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.

79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.

80) The Commission may **(…)** decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of participation in a suitable international data protection system established in third countries or a territory or a processing sector. **The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations.**

82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation (…) no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements of Articles 42 to 44 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. **The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.**

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. **They should relate in particular to compliance with the general principles relating to personal data processing, the availability of data subject's rights and effective legal remedies are available and the principles of data protection by design and by default.**

84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract, including in a contract between the processor and another processor, nor to add other clauses or additional safeguards as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

85) A corporate group or a group of enterprises engaged in a joint economic activity should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings or group of enterprises, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

87) These rules should in particular apply to data transfers required and necessary for the protection of (…) reasons of public interest, for example in cases of international data exchange, either spontaneous or on request, between competition authorities, between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health, or between competent authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent. **In the absence of an adequacy decision or of appropriate safeguards, Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.**

88) Transfers which cannot be qualified as large scale or frequent, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.

89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.

90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. (…).

91) When personal data moves across borders outside the Union it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.

107) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, **in particular on the level of protection in third countries or international organisations,** and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

Article 4

Definitions

For the purposes of this Regulation:

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

(21) ‘international organisation’ means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries;

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40

General principle for transfers

(…).

Article 41

Transfers with an adequacy decision

1. A transfer <u>of personal data to a recipient or recipients in a third country or an international organisation</u> may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any <u>specific</u> authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, <u>in particular, take account of</u> the following elements:
   (a) the rule of law, <u>respect for</u> <u>human rights and fundamental freedoms</u>, relevant legislation (…), <u>data protection</u> rules and security measures, <u>including</u> <u>rules for onward transfer of personal data to another third country or international organisation,</u> which are complied with in that country or by that international organisation, as well as <u>the existence of effective and enforceable</u> <u>data subject</u> rights <u>and</u> effective administrative and judicial redress for data subjects <u>whose personal data are being transferred</u> (…);
   (b) the existence and effective functioning of one or more independent supervisory authorities in the third country, or <u>to which an</u> international organisation <u>is subject, with responsibility</u> for ensuring compliance with the data protection rules **<u>including adequate sanctioning powers</u>** for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, **in particular** in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. **(…).** The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2).

3a. *Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission* **in accordance with the examination procedure referred to in Article 87(2). (…)**

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3). **(…)**

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or (…) processing sector within that third country, or the international organisation in question pursuant to Articles 42 to 44. (…)The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 and 5.

8. (…)

Article 42

Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a recipient or recipients in a third country or an international organisation only if the controller or processor has adduced appropriate safeguards *in a legally binding instrument* with respect to the protection of personal data **or where the controller or the processor has obtained prior authorisation for the transfer by the supervisory authority in accordance with paragraph 5.**

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:
   (a) binding corporate rules **referred to in** Article 43; or
   (b) standard data protection clauses adopted by the Commission (…) in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2); or

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority pursuant to paragraph 4; or

(e) an approved code of conduct pursuant to Article 38; or

(f) a certification mechanism pursuant to Article 39:

3. A transfer based on *binding corporate rules or standard data protection clauses* as referred to in points (a), (b) or (c) of paragraph 2 shall not require any specific authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 (…), the controller or processor shall obtain prior authorisation of the contractual clauses (…) from the competent supervisory authority (…).

5. Where, notwithstanding the requirement for a legally binding instrument in paragraph 1, appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor **(…)**shall obtain prior authorisation from the competent supervisory authority for any transfer, or category of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such a transfer (…).

5a. If the transfer referred to in paragraph 4 (…)is related to processing activities which concern data subjects in several Member States, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5b. *Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority.*

Article 43

Transfers by way of binding corporate rules

1. The competent supervisory authority shall *approve binding corporate rules* in accordance with the consistency mechanism set out in Article 58 (…) provided that they:
   (a) are legally binding and apply to, and are enforced by, every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity;
   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;
   (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall **contain a description of** at least the following elements:
   (a) the structure and contact details of the group concerned and of each of its members;
   (b) the data transfers or categories of transfers, including the types of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
   (c) their legally binding nature, both internally and externally;
   (d) application of the general data protection principles, in particular purpose limitation, including the purposes which govern further processing, data quality, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies (…) not bound by the binding corporate rules;

(e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to (…) profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Articles 14 and 14a;

(h) the tasks of any data protection officer designated in accordance with Article 35, including monitoring (…) compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;

(hh) the complaint procedures;

(i) the mechanisms within the group (…) for ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group (…), in particular by making available to the supervisory authority the results of (…) verifications of the measures referred to in point (i) of this paragraph.

[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.]

4. The Commission may specify the format and procedures for the exchange of information (…) between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 44

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 41, of appropriate safeguards pursuant to Article 42, **or of binding corporate rules pursuant to Article 43** a transfer or a category of transfers of personal data to **a recipient or recipients in** a third country or an international organisation may take place only on condition that:
   (a) the data subject has consented to the proposed transfer, after having been informed **that** such transfers **may pose** *risks* due to the absence of an adequacy decision and appropriate safeguards; or
   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
   (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer *which* is not large scale or *frequent*, is necessary for the purposes of legitimate interests pursued by the controller or the processor **which are not overridden by the interests or rights and freedoms of the data subject** and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, *where necessary*, based on this assessment adduced suitable safeguards with respect to the protection of personal data.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. (…)

4. Points (a), (b), (c) **and (h)** of paragraph 1shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the national law of the Member State to which the controller is subject. **Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.**

6. The controller or processor shall document the assessment as well as the suitable safeguards (…) referred to in point (h) of paragraph 1 in the records referred to in Article 28 (…).

6a. (…)

7. (…).

Article 45

International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
   (a) develop international co-operation mechanisms to facilitate the *effective* enforcement of legislation for the protection of personal data;
   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
   (c) engage relevant stakeholders in discussion and activities aimed at promoting international co-operation in the enforcement of legislation for the protection of personal data;
   (d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission **and supervisory authorities** shall take appropriate steps to advance the relationship with third countries and international organisations, including their supervisory authorities, in particular where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

CHAPTER VII

SECTION 3

EUROPEAN DATA PROTECTION BOARD

Article 66

Tasks of the European Data Protection Board[r]

(referred only the provisions that relate to international transfers)

1. The European Data Protection Board shall promote the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:

   (cb) give the Commission an opinion on the level of protection in third countries or international organisations, in particular in the cases referred to **in Article 41**;

   (f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

   (g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide;

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

Article 67

Reports

1. (…).

2 The European Data Protection Board *shall draw up an annual report regarding the protection of natural persons with regard to the processing of personal data in the Union and*, where relevant, *in third countries* and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission.

3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

PSEUDONIMIZZAZIONE

23) È necessario applicare i principi di protezione dei dati a tutte le informazioni relative ad una persona fisica identificata o identificabile. Per stabilire l'identificabilità di una persona, è opportuno considerare tutti i mezzi di cui può ragionevolmente avvalersi il responsabile del trattamento o un terzo per identificare detta persona direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, occorrerebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia dello sviluppo tecnologico. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono ad una persona identificata o identificabile o a dati resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, compreso per finalità statistiche e di ricerca. I principi di protezione dei dati non dovrebbero applicarsi ad una persona deceduta, a meno che le informazioni su una persona deceduta siano relative ad una persona fisica identificata o identificabile.

I dati pseudonomizzati che potrebbero essere attribuiti ad una persona fisica soltanto dall'utilizzo di ulteriori informazioni, dovrebbero essere considerati come informazioni su una persona fisica identificabile, considerando tutti i mezzi di cui può ragionevolmente avvalersi il responsabile del trattamento o qualsiasi altra persona per identificare l'interessato. I principi della protezione dei dati dovrebbero essere altresì applicati quando l'interessato può essere identificato dall'utilizzo di ulteriori informazioni, considerando tutti i mezzi di cui può ragionevolmente avvalersi il responsabile del trattamento o qualsiasi altra persona per identificare l'interessato.

39) Costituisce legittimo interesse del responsabile del trattamento *interessato* trattare dati relativi al traffico, in misura strettamente necessaria a 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, ad eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati 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. **Costituisce parimenti legittimo interesse del responsabile del trattamento interessato trattare dati personali strettamente necessari per fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.**

45) Se i dati che tratta non gli consentono di identificare una persona fisica **(...)** il responsabile del trattamento non deve essere obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione del presente regolamento (…). Tuttavia, il responsabile del trattamento non dovrebbe rifiutare le **ulteriori** informazioni fornite dall'interessato **al fine di** sostenere l'esercizio dei suoi diritti.

Articolo 4

Definizioni

Ai fini del presente regolamento s'intende per:

[...]

(3ter) **"pseudonimizzazione": il trattamento dei dati personali in modo tale da non poter essere più attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, sempre che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire la non attribuzione.**

Articolo 14 bis

Informazioni da fornire qualora i dati non siano stati ottenuti

4. I paragrafi da 1 a 3 non si applicano se e nella misura in cui:

b) comunicare tali informazioni **(...)** risulta impossibile o implicherebbe risorse sproporzionate oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento; in tali casi il responsabile del trattamento adotta misure appropriate per tutelare i legittimi interessi dell'interessato; oppure

Articolo 23

Protezione fin dalla progettazione e protezione di default

1. Tenuto conto della tecnologia disponibile e dei costi di attuazione nonché dei rischi per i diritti e le libertà delle persone fisiche costituiti dalla natura, dall'oggetto e dalla finalità del trattamento, il responsabile del trattamento (…) mette in atto (…) misure (…) tecniche e organizzative adeguate all'attività di trattamento in corso e ai suoi obiettivi, ivi incluso **la pseudonimizzazione dei dati personali,** in modo tale che il trattamento sia conforme al presente regolamento e (…) tuteli i diritti e le libertà (...) dell'interessato.

Articolo 30 ***Sicurezza del trattamento***

1. Tenuto conto della tecnologia disponibile e dei costi di attuazione, nonché della natura, del contesto, della portata e della finalità del trattamento, come anche dei rischi per i diritti e le libertà degli interessati, il responsabile del trattamento e l'incaricato del trattamento mettono in atto misure tecniche e organizzative adeguate, ivi compreso **la pseudonimizzazione dei dati personali,** per garantire un livello di sicurezza appropriato, in relazione a detti rischi.

Articolo 32

Comunicazione di una violazione dei dati personali all'interessato

3. Non è richiesta la comunicazione (…) all'interessato ai sensi del paragrafo 1 se:
   a. il responsabile del trattamento (…) ha utilizzato le opportune misure tecnologiche di protezione e (…) tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura**(...)**; oppure

Articolo 38

Codici di condotta

1 bis. Le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o incaricati del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione delle disposizioni del presente regolamento, ad esempio:

bb) la **pseudonimizzazione dei dati personali**;

_____

ALLEGATO IV

PORTABILITÀ DEI DATI PERSONALI

51) Ogni persona fisica deve avere il diritto di accedere ai dati raccolti che la riguardano e di esercitare tale diritto facilmente e ad intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai propri dati personali relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, parere di medici curanti o eventuali terapie o interventi praticati. Occorre pertanto che ogni interessato abbia il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità del trattamento, ove possibile al periodo di conservazione, ai destinatari, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e alle possibili conseguenze, almeno quando i dati si basano sul profilo dell'interessato. Tale diritto non deve ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, queste considerazioni non devono portare a negare all'interessato l'accesso a tutte le informazioni. Se il responsabile del trattamento tratta un'importante quantità di informazioni riguardanti l'interessato, il responsabile in questione può chiedere all'interessato, prima che siano fornite le informazioni, di precisare le informazioni o le attività di trattamento cui la richiesta si riferisce. **Per rafforzare ulteriormente il diritto dell'interessato di accedere ai propri dati, occorre che l'interessato abbia il diritto, se i dati personali sono trattati con mezzi elettronici e in un formato strutturato e di uso comune, di ottenere una copia dei dati che lo riguardano ugualmente in formato elettronico di uso comune.**

55) Per rafforzare ulteriormente il controllo sui propri dati **(...),** qualora il trattamento dei dati personali sia automatizzato, occorre anche che l'interessato sia autorizzato a ritirare i dati personali che ha fornito **in un formato di uso comune** da un sistema di trattamento automatizzato e trasferirli (...) ad un altro **sistema di trattamento automatizzato**.

Tale diritto dovrebbe applicarsi quando l'interessato ha fornito i dati personali al sistema di trattamento automatizzato acconsentendo al trattamento o in esecuzione di un contratto. **Non dovrebbe applicarsi quando il trattamento si basa su un altro motivo legittimo** diverso dal consenso o contratto. **Per sua natura, tale diritto non dovrebbe essere esercitato nei confronti dei responsabili del trattamento nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto segnatamente applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il responsabile del trattamento o per l'esercizio di una funzione svolta nel pubblico interesse oppure nell'esercizio di funzioni ufficiali di cui è investito il responsabile del trattamento.**

Quando, in un determinato insieme di dati personali, vi è più di un interessato, il diritto di ritirare e trasferire i dati ad un altro sistema di trattamento automatizzato non dovrebbe **pregiudicare i requisiti in materia di liceità del trattamento dei dati personali relativi ad un altro interessato in conformità del presente regolamento.**
Tale diritto non dovrebbe altresì pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali concernenti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e finché i dati siano necessari all'esecuzione di tale contratto. **(…)**

Articolo 18

Diritto alla portabilità dei dati

1. (…).

2. Se ha fornito i dati personali e il trattamento, (…) basato sul consenso o su un contratto, è effettuato in un sistema di trattamento automatizzato [fornito da un servizio della società dell'informazione], l'interessato ha il diritto di ritirare tali dati in **un formato di uso comune** e di trasmetterli in un altro sistema di trattamento automatizzato senza impedimenti da parte del responsabile del trattamento da cui sono richiamati, **fatto salvo l'articolo 17**.

2 bis. Il diritto di cui al paragrafo 2 lascia impregiudicati i diritti di proprietà intellettuale **in relazione al trattamento dei dati nei sistemi di trattamento automatizzato**.

[2ter. Il diritto di cui al paragrafo 2 non si applica al trattamento sulla base delle lettere c), d), e) e f) dell'articolo 6, paragrafo 1.]

[3. La Commissione può specificare (…) le norme tecniche, le modalità e le procedure di trasmissione dei dati personali a norma del paragrafo 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.]

4. (…).

ALLEGATO V

OBBLIGHI DEI RESPONSABILI DEL TRATTAMENTO E DEGLI INCARICATI DEL TRATTAMENTO

63bis) Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che l'incaricato del trattamento deve eseguire per conto del responsabile del trattamento, quando affida delle attività di trattamento a un incaricato del trattamento, il responsabile del trattamento dovrebbe ricorrere unicamente a incaricati del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che saranno conformi al presente regolamento, incluso per la sicurezza del trattamento. Tali garanzie sufficienti possono essere dimostrate tramite l'adesione dell'incaricato del trattamento ad un codice di condotta o ad un meccanismo di certificazione. L'esecuzione dei trattamenti su commissione dovrebbe essere disciplinata da un contratto o da altro atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento, in cui siano stipulati la materia disciplinata e la durata del contratto, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici dell'incaricato del trattamento nel contesto del trattamento da eseguire e dei rischi per i diritti e le libertà dell'interessato. Il responsabile del trattamento e l'incaricato del trattamento possono scegliere di usare un contratto individuale o clausole contrattuali tipo che sono adottate dalla Commissione o da un'autorità di controllo in conformità del meccanismo di coerenza e adottate dalla Commissione, o che sono parte di una certificazione garantita nel meccanismo di certificazione. L'incaricato del trattamento che tratta i dati personali diversamente da quanto indicato nelle istruzioni del responsabile del trattamento è considerato responsabile del trattamento per tale trattamento. Dopo il completamento del trattamento per conto del responsabile del trattamento, l'incaricato del trattamento dovrebbe restituire o cancellare i dati personali salvo che il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento preveda un requisito di conservazione dei dati; in tal caso l'incaricato del trattamento dovrebbe mettere in atto misure adeguate per garantire la sicurezza e riservatezza dei dati personali e dovrebbe astenersi dal trattare di propria iniziativa tali dati.

Articolo 26

Incaricato del trattamento

1. Il responsabile del trattamento ricorre unicamente a incaricati del trattamento che presentino garanzie sufficienti per mettere in atto misure (…) tecniche e organizzative adeguate in modo tale che il trattamento sia conforme al presente regolamento (…).

1 bis. La presentazione di garanzie sufficienti, prevista ai paragrafi 1 e 2bis può essere dimostrata tramite l'adesione **dell'incaricato del trattamento** a un codice di condotta, di cui all'articolo 38, o un meccanismo di certificazione, di cui all'articolo 39.

2. L'esecuzione dei trattamenti su commissione è disciplinata da un contratto o da altro atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento,in cui sono stipulati la materia disciplinata e la durata del contratto, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati e che preveda segnatamente che l'incaricato del trattamento:

a) **agisca soltanto su istruzione del responsabile del trattamento (…), salvo che lo richieda il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento e, in tal caso, l'incaricato del trattamento notifica il responsabile del trattamento a meno che il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento vieti tale notifica per rilevanti motivi di interesse pubblico;**

b) (…).

c) prenda tutte le misure richieste ai sensi dell'articolo 30;

d) stabilisca le condizioni per ricorrere ad un altro incaricato del trattamento (…), come un requisito di consenso preventivo specifico del responsabile del trattamento;

e) per quanto possibile tenuto conto della natura del trattamento, assista il responsabile del trattamento nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) determini come il responsabile del trattamento deve essere aiutato a garantire il rispetto degli obblighi di cui agli articoli da 30 a 34;

g) restituisca o cancelli, a scelta del responsabile del trattamento, i dati personali dopo il completamento del trattamento precisato nel contratto o altro atto giuridico, salvo che il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento preveda un requisito di conservazione dei dati; in tal caso l'incaricato del trattamento mette in atto misure adeguate per garantire la sicurezza e riservatezza dei dati personali;

h) metta a disposizione del responsabile del trattamento (…) tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo.

2 bis. Quando un incaricato del trattamento ricorre ad un altro incaricato del trattamento per l'esecuzione di specifiche attività di trattamento per conto del responsabile del trattamento, l'altro incaricato del trattamento presenta garanzie sufficienti per mettere in atto misure (…) tecniche e organizzative adeguate in modo tale che il trattamento sia conforme al presente regolamento.

2 bis bis. Quando un incaricato del trattamento ricorre ad un altro incaricato del trattamento per l'esecuzione di specifiche attività di trattamento per conto del responsabile del trattamento, in un contratto o altro atto giuridico sono imposti gli stessi obblighi su tale altro incaricato del trattamento come stabilito nel contratto o altro atto giuridico tra il responsabile del trattamento e l'incaricato del trattamento di cui al paragrafo 2.

2 bis ter. Fatto salvo un contratto individuale tra il responsabile del trattamento e l'incaricato del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 2 e 2 bis bis può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 2 ter e 2 quater o su clausole contrattuali tipo che sono parte di una certificazione concessa al responsabile del trattamento o all'incaricato del trattamento ai sensi degli articoli 39 e 39 bis.

2 ter. La Commissione può stabilire clausole contrattuali tipo per le materie di cui al paragrafo 2 e in conformità della procedura d'esame di cui all'articolo 87, paragrafo 2.

2 quater. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui al paragrafo 2 e in conformità del meccanismo di coerenza di cui all'articolo 57.

3. Il contratto o altro atto giuridico cui si fa riferimento ai paragrafi 2 e 2bis sono tenuti in forma scritta, o elettronica o in qualunque altro formato non leggibile ma convertibile in un formato leggibile.

4. (…).

5. (…).