

Relazione annuale

2010



GARANTE EUROPEO
DELLA PROTEZIONE DEI DATI



Relazione annuale

2010



Europe Direct è un servizio a vostra disposizione per aiutarvi a trovare le risposte ai vostri interrogativi sull'Unione europea.

Numero verde unico (*):

00 800 6 7 8 9 10 11

(*) Alcuni gestori di telefonia mobile non consentono l'accesso ai numeri 00 800 o non ne accettano la gratuità.

Numerose altre informazioni sull'Unione europea sono disponibili su Internet consultando il portale Europa (<http://europa.eu>).

Una scheda catalografica figura alla fine del volume.

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2010

ISBN 978-92-95073-22-7

doi:10.2804/21740

© Unione europea, 2011

Riproduzione autorizzata con citazione della fonte.

© Fotografie: Parlamento europeo e iStockphoto

Printed in Luxembourg

STAMPATO SU CARTA SBIANCATA SENZA CLORO ELEMENTARE (ECF)

Indice

1 PUNTI SALIENTI DEL 2010

2 CONTROLLO E APPLICAZIONE DELLA LEGGE

3 CONSULTAZIONE

Guida per gli utenti	7
Definizione del mandato	9
Premessa	11
1. PUNTI SALIENTI DEL 2010	12
1.1. Caratteristiche essenziali	12
1.2. Quadro generale del 2010	13
1.3. Risultati del 2010	16
2. CONTROLLO E APPLICAZIONE DELLA LEGGE	18
2.1. Introduzione	18
2.2. Responsabili della protezione dei dati	18
2.3. Controlli preventivi	20
2.3.1. Base giuridica	20
2.3.2. Procedura	20
2.3.3. Questioni principali trattate nell'ambito dei controlli preventivi	23
2.3.4. Consultazioni sulla necessità di controlli preventivi	29
2.3.5. Notifiche non soggette a controllo preventivo o ritirate	29
2.3.6. Seguito dato ai pareri di controllo preventivo	29
2.3.7. Conclusioni	30
2.4. Reclami	30
2.4.1. Il mandato del GEPD	30
2.4.2. Procedura per la gestione dei reclami	31
2.4.3. Garanzia di riservatezza agli autori dei reclami	33
2.4.4. Reclami esaminati nel corso del 2010	34
2.4.5. Altre attività nel campo dei reclami	36
2.5. Controllo di conformità	38
2.5.1. Controllo mirato ed esercizi di rendicontazione	38
2.5.2. Controllo e rendicontazione generale: esercizio "Primavera 2009"	39
2.5.3. Prossimi passi	39
2.5.4. Ispezioni	40
2.6. Consultazioni su misure amministrative	42
2.6.1. Consultazioni ai sensi degli articoli 28, paragrafo 1, e 46, lettera d)	42
2.6.2. Richiesta di accesso all'identità di un informatore – Mediatore europeo	42
2.6.3. Trasferimenti internazionali di dati personali – Agenzia europea per la sicurezza aerea	42
2.6.4. Politica sull'uso interno della posta elettronica – Commissione europea	43
2.6.5. Diritti dell'amministratore informatico – Banca europea per gli investimenti	43
2.6.6. Controllo delle comunicazioni telefoniche	43
2.6.7. Trattamento successivo di dati per trasferimenti all'AMEX – Autorità europea per la sicurezza alimentare	44
2.6.8. Periodi di conservazione dei documenti sanitari – Collegio dei capi dell'amministrazione	45
2.6.9. Norme di applicazione riguardanti il responsabile della protezione dei dati	46
2.7. Orientamenti tematici	46
2.7.1. Orientamenti per indagini amministrative e procedimenti disciplinari	46
2.7.2. Orientamenti sulla videosorveglianza	47
2.8. La politica del GEPD di conformità e applicazione delle norme	48
3. CONSULTAZIONE	50
3.1. Introduzione: panoramica degli sviluppi e delle tendenze principali	50
3.2. Quadro politico e priorità	51
3.2.1. Attuazione della politica di consultazione	51
3.2.2. Risultati del 2010	52
3.3. Revisione del quadro comunitario di protezione dei dati	53
3.4. Spazio di libertà, sicurezza e giustizia	54
3.4.1. Strategia di sicurezza interna dell'UE	54
3.4.2. Gestione delle informazioni	54

3.4.3. Frontex	55
3.4.4. Politica antiterrorismo	55
3.4.5. Immissione sul mercato e uso di precursori di esplosivi	55
3.4.6. Regolamento Eurodac	56
3.4.7. Abusi sessuali di minori e pedopornografia	56
3.4.8. Ordine di protezione europeo e ordine europeo di indagine penale	57
3.5. e-Privacy e tecnologia	57
3.5.1. Promuovere la fiducia nella società dell'informazione	57
3.5.2. Internet e neutralità della rete	58
3.5.3. Direttiva sulla conservazione dei dati	58
3.5.4. Rifiuti elettronici	59
3.5.5. Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)	60
3.5.6. Giustizia elettronica	60
3.5.7. Settimo programma quadro di RST, compreso il progetto Turbine	60
3.6. Cooperazione internazionale e trasferimenti di dati	61
3.6.1. Dati dei passeggeri contenuti nel codice di prenotazione	61
3.6.2. Programma di controllo delle transazioni finanziarie dei terroristi	62
3.6.3. Accordo internazionale UE-USA sulla condivisione delle informazioni e la protezione dei dati personali	62
3.6.4. Accordo commerciale anticontraffazione	63
3.7. Fiscalità e dogane	64
3.7.1. Cooperazione nel settore fiscale	64
3.7.2. Cooperazione doganale UE-Giappone	64
3.8. Accesso del pubblico, inclusi i procedimenti giurisdizionali relativi	65
3.8.1. Accesso del pubblico a documenti contenenti dati personali	65
3.8.2. Altri procedimenti giudiziari	65
3.9. Altre questioni	66
3.9.1. Sistema d'informazione del mercato interno	66
3.9.2. Body scanner	66
3.9.3. Sistemi di garanzia dei depositi	66
3.9.4. Iniziativa dei cittadini	67
3.9.5. Indagine e prevenzione di incidenti e inconvenienti nell'aviazione civile	67
3.10. Uno sguardo al futuro	68
3.10.1. Il progresso tecnologico	68
3.10.2. Priorità per il 2011	69



4. COOPERAZIONE	70
4.1. Gruppo di lavoro Articolo 29	70
4.2. Controllo coordinato di Eurodac	71
4.3. Controllo del sistema d'informazione doganale (SID)	73
4.4. Cooperazione di polizia e giudiziaria: cooperazione con OCC/ACC e GLPG	73
4.5. Conferenza europea	74
4.6. Conferenza internazionale	74
4.7. Organizzazioni internazionali (Seminario di Firenze)	75



5. COMUNICAZIONE	76
5.1. Introduzione	76
5.2. "Caratteristiche" della comunicazione	76
5.2.1. Pubblico e gruppi di riferimento	76
5.2.2. Politica linguistica	77
5.3. Rapporti con i media	77
5.3.1. Comunicati stampa	77
5.3.2. Interviste	77
5.3.3. Conferenze stampa	78
5.3.4. Richieste dei media	78
5.4. Richieste di informazioni e pareri	79
5.5. Visite di studio	80
5.6. Strumenti d'informazione online	81
5.6.1. Sito Internet	81
5.6.2. Newsletter	81
5.6.3. Intranet	82

5.7. Pubblicazioni	82
5.7.1. Relazione annuale	82
5.7.2. Pubblicazioni tematiche	82
5.8. Eventi di sensibilizzazione	83
5.8.1. Giornata della protezione dei dati	83
5.8.2. Giornata Porte aperte dell'Unione europea	84

6 AMMINISTRAZIONE, BILANCIO E PERSONALE

6. AMMINISTRAZIONE, BILANCIO E PERSONALE	86
6.1. Introduzione	86
6.2. Bilancio	86
6.3. Risorse umane	87
6.3.1. Assunzioni	87
6.3.2. Programma di tirocinio	88
6.3.3. Programma per gli esperti nazionali distaccati	88
6.3.4. Organigramma	89
6.3.5. Formazione	89
6.3.6. Attività sociali	89
6.4. Funzioni di controllo	90
6.4.1. Controllo interno	90
6.4.2. Audit interno	90
6.4.3. Sicurezza	90
6.5. Infrastrutture	90
6.6. Contesto amministrativo	91
6.6.1. Assistenza amministrativa e cooperazione interistituzionale	91
6.6.2. Norme interne	92
6.6.3. Gestione dei documenti	92

7 IL RESPONSABILE DELLA PROTEZIONE DEI DATI PRESSO IL GEPD

7. IL RESPONSABILE DELLA PROTEZIONE DEI DATI PRESSO IL GEPD	94
7.1. Un nuovo gruppo dell'RPD presso il GEPD	94
7.2. Piano d'azione e norme di applicazione	94
7.3. Un registro delle operazioni di trattamento facilmente accessibile	94
7.4. Esercizio di primavera	95
7.5. Informazione e sensibilizzazione	95

8 PRINCIPALI OBIETTIVI PER IL 2011

8. PRINCIPALI OBIETTIVI PER IL 2011	96
8.1. Controllo e applicazione della legge	96
8.2. Politica e consultazione	96
8.3. Altri campi	97

Allegato A — Quadro giuridico	98
Allegato B — Estratto dal regolamento (CE) n. 45/2001	100
Allegato C — Elenco delle abbreviazioni	102
Allegato D — Elenco dei responsabili della protezione dei dati	104
Allegato E — Elenco dei pareri su controlli preventivi	107
Allegato F — Elenco dei pareri su proposte legislative	111
Allegato G — Discorsi del Garante e del Garante aggiunto	113
Allegato H — Organigramma del segretariato del GEPD	116

GUIDA PER GLI UTENTI

La presente guida è seguita da una definizione del mandato e da una premessa del sig. Peter Hustinx, Garante europeo della protezione dei dati (GEPD), e del sig. Giovanni Buttarelli, Garante aggiunto.

Il **Capitolo 1 — Punti salienti del 2010** presenta le principali caratteristiche del lavoro svolto dal GEPD nel 2010 e i risultati raggiunti nei vari campi di attività.

Il **Capitolo 2 — Controllo** descrive quanto è stato fatto per assicurare e controllare che le istituzioni e gli organismi dell'UE assolvano i loro obblighi in materia di protezione dei dati. Questo capitolo presenta un'analisi delle principali questioni relative ai controlli preventivi, l'ulteriore lavoro nel campo dei reclami, la verifica del rispetto della normativa e la consulenza sulle misure amministrative trattate nel 2010. Contiene inoltre gli orientamenti tematici adottati dal GEPD nei settori delle indagini amministrative e dei procedimenti disciplinari, nonché l'ulteriore lavoro sugli orientamenti per la videosorveglianza. Il capitolo presenta altresì la nuova politica del GEPD sulla conformità e l'applicazione delle norme.

Il **Capitolo 3 — Consultazione** è dedicato all'evoluzione del ruolo consultivo del GEPD ed è incentrato sui pareri e sulle osservazioni emessi in riferimento a proposte legislative e ai relativi documenti, nonché sul loro impatto in un numero crescente di settori. Il capitolo affronta inoltre il coinvolgimento del GEPD in cause discusse di fronte alla Corte di giustizia e contiene un'analisi di tematiche orizzontali: talune nuove questioni tecnologiche e nuovi sviluppi in campo politico e legislativo.

Il **Capitolo 4 — Cooperazione** descrive il lavoro svolto in alcune sedi importanti, quali il gruppo di lavoro Articolo 29 per la protezione dei dati e le conferenze europea e internazionale sulla protezione dei dati. Il capitolo si occupa inoltre del controllo coordinato (da parte del GEPD e delle autorità nazionali competenti per la protezione dei dati) di sistemi informatici su larga scala.

Il **Capitolo 5 — Comunicazione** presenta le attività d'informazione e comunicazione del GEPD e i relativi risultati, nonché la comunicazione esterna con i media, eventi di

sensibilizzazione, l'informazione al pubblico e gli strumenti d'informazione online.

Il **Capitolo 6 — Amministrazione, bilancio e personale** descrive dettagliatamente i principali sviluppi in seno all'organizzazione del GEPD, incluse le questioni riguardanti il bilancio e le risorse umane nonché gli accordi amministrativi.

Il **Capitolo 7 — Responsabile della protezione dei dati (RPD) del GEPD** presenta l'attività del nuovo gruppo di lavoro RPD del GEPD. Facendo riferimento al piano d'azione dell'RPD e alle regole di applicazione adottate, il capitolo illustra lo stato di avanzamento del registro dei trattamenti notificati, la conformità all'esercizio di primavera e l'esigenza di informare e sensibilizzare.

Il **Capitolo 8 — Obiettivi principali nel 2011** fornisce una breve anticipazione e le principali priorità per il 2011.

La relazione è completata da una serie di **allegati** che offrono una panoramica del quadro normativo di riferimento e comprendono le disposizioni del regolamento (CE) n. 45/2001, l'elenco dei responsabili della protezione dei dati, gli elenchi dei pareri emessi dal GEPD nell'ambito dei controlli preventivi e dei pareri consultivi, i discorsi pronunciati dal Garante e dal Garante aggiunto e la composizione del segretariato del GEPD.

È inoltre disponibile una sintesi della presente relazione, intesa a fornire una rapida visione d'insieme dei principali sviluppi delle attività del GEPD nel 2010.

Per maggiori informazioni sul GEPD si prega di consultare il sito Internet all'indirizzo <http://www.edps.europa.eu>, sul quale è presente anche una funzione per abbonarsi alla nostra newsletter.

Versioni cartacee della relazione annuale e della sintesi possono essere ordinate gratuitamente presso l'EU Bookshop, la libreria elettronica dell'Unione europea, (<http://www.bookshop.europa.eu>).

DEFINIZIONE DEL MANDATO

Il Garante europeo della protezione dei dati (GEPD) ha il compito di garantire il rispetto dei diritti e delle libertà fondamentali delle persone, con particolare riguardo alla vita privata, da parte delle istituzioni e degli organismi dell'Unione europea quando procedono al trattamento di dati personali.

Il GEPD ha il compito di:

- controllare e assicurare il rispetto delle disposizioni del regolamento (CE) n. 45/2001 ⁽¹⁾ e di qualunque altro atto comunitario relativo alla tutela dei diritti e delle libertà fondamentali quando le istituzioni e gli organismi dell'Unione europea trattano dati personali (controllo);
- fornire consulenza alle istituzioni e agli organismi dell'Unione europea su tutte le questioni relative al trattamento di dati personali, ivi compresa la consulenza su proposte legislative e il controllo di nuovi sviluppi che hanno implicazioni per la protezione dei dati personali (consulenza);
- collaborare con le autorità nazionali di controllo e con gli organi di controllo nel quadro dell'ex "terzo pilastro" dell'UE, per rendere più coerente la protezione dei dati personali (cooperazione).

In tal senso, il GEPD punta strategicamente:

- alla promozione di una "cultura della protezione dei dati" nelle istituzioni e negli organismi, contribuendo in tal modo a migliorare la buona governance;
- all'integrazione del rispetto dei principi di protezione dei dati nella legislazione e nelle politiche comunitarie, ove opportuno;
- al miglioramento della qualità delle politiche comunitarie, nella misura in cui la protezione effettiva dei dati costituisca una condizione di base per il successo di dette politiche.

⁽¹⁾ Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, 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 (GU L 8 del 12.1.2001, pag. 1).

PREMESSA



Siamo lieti di presentare la relazione annuale delle attività del Garante europeo della protezione dei dati (GEPD) al Parlamento europeo, al Consiglio e alla Commissione europea, in conformità del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio e dell'articolo 16 del trattato sul funzionamento dell'Unione europea, che ha sostituito l'articolo 286 del trattato CE.

La presente relazione riguarda il 2010, il sesto anno completo di attività dall'istituzione del GEPD quale nuovo organo indipendente di controllo incaricato di garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riguardo alla vita privata, in merito al trattamento dei dati personali da parte delle istituzioni e degli organismi dell'UE. La relazione riguarda altresì il secondo anno del nostro mandato comune di cinque anni in qualità di membri di questa autorità.

Anche il 2010 è stato un anno molto importante per il diritto fondamentale alla protezione dei dati. Il trattato di Lisbona, che assicura una solida base giuridica per una protezione dei dati completa in tutte le aree della politica dell'UE, ha avuto un impatto sempre più visibile. Il processo di revisione del quadro giuridico dell'UE per la protezione dei dati sta prendendo forma e attira un'attenzione crescente. Due programmi politici decisivi – il programma di Stoccolma nello spazio di libertà, sicurezza e giustizia e l'agenda digitale, pietra angolare della strategia Europa 2020 – dimostrano l'importanza della protezione dei dati quale elemento cruciale della legittimità e dell'efficacia in entrambi i settori.

Il GEPD ha profuso un grande impegno in questi contesti differenti ed è determinato a proseguire in tal senso anche nel prossimo futuro. Al contempo, ci siamo assicurati che il ruolo di autorità indipendente di controllo venisse svolto in tutte le principali aree di attività e che la sua organizzazione fosse del tutto adeguata. Ciò ha prodotto un progresso significativo sia del controllo delle istituzioni e degli organismi dell'UE durante il trattamento dei dati personali e della consulenza su nuove misure politiche e legislative, sia della stretta cooperazione con altre autorità di controllo per assicurare maggiore uniformità nella protezione dei dati.

Desideriamo pertanto cogliere l'opportunità di ringraziare coloro i quali, in seno al Parlamento europeo, al Consiglio e alla Commissione, sostengono il nostro lavoro, nonché tutte le altre persone che, nei vari organismi e istituzioni, sono responsabili delle modalità concrete di attuazione della protezione dei dati. Desideriamo altresì incoraggiare tutti coloro che si stanno occupando delle importanti sfide future.

Infine, rivolgiamo un ringraziamento speciale ai membri del nostro personale, che danno prova di qualità eccezionali e contribuiscono in larga misura alla nostra efficacia.

Peter Hustinx
Garante europeo della protezione dei dati

Giovanni Buttarelli
Garante aggiunto

1

PUNTI SALIENTI DEL 2010

1.1. Caratteristiche essenziali

Alcuni sviluppi recenti hanno contribuito a collocare **i diritti fondamentali e la protezione dei dati** al centro dell'agenda europea. Il **trattato di Lisbona**, in vigore dal 1° dicembre 2009, ha accresciuto l'importanza dei diritti fondamentali nell'Unione europea (UE) attribuendo alla Carta dei diritti fondamentali lo stesso valore legale dei trattati e incaricando l'UE di aderire alla **Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali** (ECHR). Specificamente in materia di protezione dei dati, l'articolo 16 TFUE fornisce una base giuridica generale per la tutela delle persone fisiche riguardo al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari e degli Stati membri dell'UE durante l'esecuzione delle attività che rientrano nel campo di applicazione della legislazione comunitaria.

L'importanza dei diritti fondamentali in generale e della protezione dei dati in particolare è ulteriormente sottolineata dal **programma di Stoccolma**, l'attuale programma politico quinquennale nello spazio di libertà, sicurezza e giustizia. Il programma evidenzia la necessità di garantire il rispetto dei diritti fondamentali, della libertà e dell'integrità delle persone assicurando nel contempo la sicurezza. Conseguentemente, il rispetto dei diritti umani e della dignità nonché degli altri diritti sanciti dalla Carta e dall'ECHR – in particolare il diritto alla vita privata e alla protezione dei dati – è un valore centrale dell'azione dell'Europa in questo campo. È significativo che il Consiglio europeo abbia invitato la Commissione a sottoporre "con urgenza" una proposta per l'adesione dell'Unione all'ECHR.

Questi sviluppi hanno avuto il sostegno anche da parte di altre istituzioni. In relazione al programma di Stoccolma, il Parlamento europeo ha significativamente sottolineato il ruolo dei diritti fondamentali per lo sviluppo futuro dello spazio di libertà, sicurezza e giustizia ⁽²⁾. La Commissione ha adottato di recente una comunicazione che delinea una strategia per l'effettiva applicazione della Carta nel nuovo quadro giuridico creatosi con l'entrata in vigore del trattato di Lisbona.

Il **processo di revisione del quadro della protezione dei dati** avviato nel 2009 e portato avanti nel 2010 costituisce un elemento decisivo di un'Europa dei diritti fondamentali. Nel novembre 2010 la Commissione ha pubblicato una comunicazione che delinea un approccio globale alla protezione dei dati personali nell'Unione europea. La comunicazione stabilisce l'approccio della Commissione alla modernizzazione del quadro giuridico comunitario per la protezione dei dati personali in tutte le aree di attività dell'Unione. La comunicazione mira altresì ad affrontare le sfide conseguenti alla globalizzazione e alle nuove tecnologie in modo tale da garantire in futuro un elevato livello di protezione dei dati. Il GEPD segue da vicino il processo di revisione e vi ha già contribuito in diverse fasi. Questo progetto sarà una delle nostre massime priorità anche nel 2011.

⁽²⁾ Risoluzione del Parlamento europeo del 25 novembre 2009 sulla comunicazione della Commissione – Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini – Programma di Stoccolma, P7_TA(2009)0090.

Nel 2010 la Commissione ha profuso un notevole impegno anche nell'attuazione delle varie iniziative collegate al programma di Stoccolma. Molte di queste proposte si fondano su un intenso scambio di dati tra le autorità preposte all'applicazione della legge o le autorità di pubblica sicurezza dei vari paesi e hanno pertanto un impatto reale sulla vita privata e sulla protezione dei dati delle persone. In sede di sviluppo dello **spazio di libertà, sicurezza e giustizia**, il potere legislativo europeo deve costantemente trovare un equilibrio tra la sicurezza e la libertà di circolazione dei cittadini e la protezione della loro vita privata e dei loro dati personali. L'attuazione del programma di Stoccolma ha rappresentato un elemento essenziale delle attività del GEPD nel 2010 e tutto lascia pensare che sarà così anche in futuro.

Un'altra caratteristica importante del 2010 riguarda gli aspetti della protezione dei dati che sono correlati alle **nuove tecnologie**. Le tecnologie disponibili attualmente permettono uno scambio e un trattamento di dati di proporzioni mai viste prima. Allo stesso tempo, il trattamento dei dati è diventato più astuto e più difficile da scoprire: reti sociali, cloud computing, raccolta dei pedaggi stradali, dispositivi di geolocalizzazione, pubblicità comportamentale e altri servizi simili rappresentano sfide enormi per la protezione dei dati. La revisione del quadro della protezione dei dati dovrà confrontarsi in maniera efficace con tutte queste sfide per assicurare una protezione d'alto livello dei dati personali in un mondo guidato dalla tecnologia. Le nuove tecnologie sono inoltre al centro delle iniziative previste dall'agenda digitale della Commissione per l'Europa. Il GEPD prenderà in esame tali iniziative e le valuterà, ogniqualvolta esse abbiano implicazioni per la protezione dei dati delle persone.

1.2. Quadro generale del 2010

Le principali attività svolte dal GEPD nel corso del 2010 si sono basate sulla stessa strategia generale degli anni precedenti, però hanno continuato a crescere in quantità e in portata. È stata pertanto migliorata la capacità di azione del GEPD in termini sia di efficienza che di efficacia.

Il quadro giuridico ⁽³⁾ nel quale il GEPD opera definisce una serie di compiti e di competenze che permettono di distinguere tre ruoli principali. Essi continuano a fungere da piattaforme strategiche delle

⁽³⁾ Cfr. la panoramica del quadro giuridico nell'allegato A e l'estratto dal regolamento (CE) n. 45/2001 nell'allegato B.

attività del GEPD e sono indicati anche nella descrizione della sua missione:

- **un ruolo di controllo**, che consiste nel sorvegliare e garantire che le istituzioni e gli organismi dell'UE ⁽⁴⁾ rispettino le tutele giuridiche esistenti ogniqualvolta trattano dati personali;
- **un ruolo consultivo**, che consiste nel fornire consulenza alle istituzioni e agli organismi dell'UE su tutte le questioni pertinenti e, in particolare, sulle proposte legislative che hanno implicazioni per la protezione dei dati personali;
- **un ruolo di cooperazione**, che consiste nel collaborare con le autorità e gli organismi nazionali di controllo nel contesto dell'ex terzo pilastro dell'Unione europea e comprende la collaborazione di polizia e giudiziaria in materia penale, al fine di migliorare la coerenza della protezione dei dati personali.

La descrizione di questi ruoli sarà ulteriormente ampliata nei capitoli 2, 3 e 4 della presente relazione annuale, dove sono descritti le principali attività del GEPD e i progressi compiuti nel 2010. Alcuni elementi essenziali sono sintetizzati in questa sezione.

L'importanza dell'informazione e della comunicazione in merito a queste attività è tale da giustificare pienamente una trattazione separata nel capitolo 5 del tema della comunicazione. Tutte queste attività si fondano su una gestione efficace delle risorse finanziarie, umane e d'altro tipo, come illustrato nel capitolo 6.

Controllo

I compiti di controllo spaziano dalla consulenza e dal sostegno ai responsabili della protezione dei dati, passando attraverso il controllo preventivo di operazioni di trattamento dati rischiose, fino alla conduzione di indagini, comprese le ispezioni in loco e la gestione dei reclami. Ulteriore consulenza all'amministrazione dell'UE può avvenire attraverso consultazioni su misure amministrative o la pubblicazione di orientamenti tematici.

⁽⁴⁾ I termini "istituzioni" e "organismi" di cui al regolamento (CE) n. 45/2001 sono usati in tutta la relazione e comprendono anche le agenzie dell'Unione europea. Per un elenco completo, consultare il link seguente: http://europa.eu/agencies/community_agencies/index.en.htm

Tutte le istituzioni e gli organismi comunitari devono avere almeno un **responsabile della protezione dei dati** (RPD). Nel 2010 il numero totale degli RPD è salito a 47. Un'interazione costante con gli RPD e la loro rete è una condizione importante per garantire un controllo efficace. È stato istituito un "quartetto di RPD", formato da quattro RPD (del Consiglio, del Parlamento europeo, della Commissione europea e del Centro di traduzione degli organismi dell'Unione europea), con il compito di coordinare la rete degli RPD. Il GEPD ha collaborato strettamente con il quartetto.

Anche nel 2010, il **controllo preventivo** delle operazioni di trattamento dati rischiose ha costituito la parte principale delle attività di controllo. Il GEPD ha adottato 55 pareri di controllo preventivo sulle procedure amministrative standard, come la valutazione del personale, assunzioni e promozioni, ma anche sulle attività operative centrali, quali il sistema di allarme rapido e di reazione per lo scambio di informazioni su malattie trasmissibili. I relativi pareri sono pubblicati sul sito del GEPD e la loro attuazione è seguita sistematicamente.

L'**applicazione del regolamento** da parte delle istituzioni e degli organismi comunitari è anch'essa oggetto di controlli sistematici mediante rilevamenti periodici dei valori degli indicatori di prestazione che riguardano tutte le istituzioni e tutti gli organismi dell'UE. Facendo seguito all'esercizio generale di controllo avviato nella primavera del 2009, il GEPD ha continuato a vigilare sull'applicazione delle norme e dei principi in materia di protezione dei dati da parte delle istituzioni e degli organismi interessati. Il prossimo esercizio generale (primavera 2011) comincerà all'inizio del 2011. Sono stati condotti anche esercizi di verifica mirati laddove, a seguito delle attività di controllo, il GEPD ha ritenuto che il livello di conformità di determinati organismi o istituzioni fosse allarmante. Parte di questi controlli è avvenuta per via epistolare, altri sotto forma di visite all'organismo interessato. Nel 2010 il GEPD ha effettuato due visite di questo tipo, oltre a un'ispezione in loco presso il Centro comune di ricerca della Commissione a Ispra, per verificare la conformità riguardo a questioni specifiche.

Nel 2010 il numero totale di **reclami** è stato pari a 94; di essi, 25 sono stati giudicati ammissibili. Molti reclami inammissibili riguardavano questioni di livello nazionale che non rientrano nelle competenze del GEPD. La maggior parte delle questioni sollevate nei reclami giudicati ammissibili riguardavano presunte violazioni del diritto di accesso e rettificazione, l'uso illegittimo, la raccolta eccessiva

e la cancellazione di dati. In undici casi il GEPD ha concluso che c'era stata una violazione delle norme sulla protezione dei dati.

Ulteriore lavoro è stato compiuto in forma di **consulenza sulle misure amministrative** previste dalle istituzioni e dagli organismi dell'UE in riferimento al trattamento dei dati personali. Sono state sollevate varie questioni, tra cui i trasferimenti internazionali di dati, l'accesso all'identità di un informatore, l'utilizzo interno della posta elettronica e il monitoraggio elettronico.

Il GEPD ha inoltre adottato **orientamenti** riguardanti indagini amministrative e procedimenti disciplinari e la videosorveglianza.

Nel dicembre 2010 il GEPD ha adottato un documento politico dal titolo "Controllare e garantire la conformità al regolamento (CE) n. 45/2001", che delinea il quadro entro il quale il GEPD controlla, misura e garantisce la conformità alla protezione dei dati da parte dell'amministrazione comunitaria. Il documento illustra altresì i vari **poteri di applicazione delle norme** di cui il GEPD dispone e riporta i motivi e le circostanze per i quali e nelle quali il Garante può adottare azioni formali.

Consultazione

Nel 2010 la Commissione ha compiuto progressi significativi verso un **quadro giuridico nuovo e aggiornato per la protezione dei dati in Europa**. La consultazione pubblica lanciata nel 2009 si è conclusa ed è stata integrata da un'ulteriore consultazione mirata con alcune delle principali parti interessate. Nel novembre 2010 la Commissione ha pubblicato la comunicazione che delinea un approccio globale alla protezione dei dati personali nell'Unione europea e individua le principali priorità e gli obiettivi chiave per la revisione delle regole vigenti.

Il GEPD ha riservato un'attenzione speciale al processo di revisione durante tutto il 2010 e ha diffuso i propri messaggi in molti modi. In particolare, ha tenuto una conferenza ad hoc subito dopo la pubblicazione della comunicazione, per esprimere pubblicamente le proprie opinioni sul nuovo quadro giuridico. In tale occasione, il GEPD ha sottolineato l'importanza della revisione, che ha giudicato molto tempestiva, e ha fornito il proprio orientamento sui punti principali del nuovo quadro giuridico.

Il GEPD ha continuato ad attuare la propria **politica di consultazione generale** e ha emesso un

numero record di pareri legislativi – 19 – su argomenti diversi. Questa politica fornisce anche un approccio proattivo che comprende un inventario regolare di proposte legislative da sottoporre a consultazione e la disponibilità a commenti informali nelle fasi preparatorie delle proposte legislative. La maggior parte dei pareri del GEPD sono stati oggetto di follow-up in forma di discussioni con il Parlamento europeo e il Consiglio.

Nel 2010 il GEPD ha seguito da vicino numerose iniziative direttamente collegate all'attuazione del **programma di Stoccolma**. Tra l'altro, il GEPD ha affrontato questioni cruciali di protezione dei dati correlate alla strategia di sicurezza interna dell'UE, alla gestione delle informazioni nello spazio di libertà, sicurezza e giustizia, alla politica antiterrorismo dell'UE e ai regolamenti di Frontex ed Eurodac. Tutto considerato, gli sviluppi del programma di Stoccolma sono stati un tema dominante nell'agenda del GEPD e continueranno a esserlo anche negli anni a venire.

Il GEPD è intervenuto in maniera significativa anche in riferimento all'**interfaccia tra la tutela della vita privata e gli sviluppi tecnologici**. Nel maggio 2010 la Commissione ha pubblicato la comunicazione su un'agenda digitale per l'Europa, allo scopo di fissare le priorità dell'UE riguardo a Internet e alle tecnologie digitali. Nel marzo 2010 il GEPD ha adottato un parere sulla promozione della fiducia nella società dell'informazione attraverso l'incentivazione della protezione dei dati e della vita privata, a titolo di contributo a questa strategia digitale. È inoltre intervenuto in vari modi su iniziative riguardanti Internet e la neutralità della rete, la revisione della direttiva sulla conservazione dei dati, la direttiva sui rifiuti elettronici, il regolamento ENISA e la giustizia elettronica.

Il GEPD è stato consultato anche riguardo a varie iniziative nel campo della **cooperazione internazionale in materia di sicurezza e applicazione della legge**, come l'accordo generale tra l'Unione europea e gli Stati Uniti d'America sulla condivisione di dati ai fini dell'applicazione della legge e l'accordo sullo scambio di dati finanziari nell'ambito del programma di controllo delle transazioni finanziarie dei terroristi (TFTP II); è intervenuto altresì in relazione all'accordo commerciale anticontraffazione (ACTA) e agli accordi sullo scambio dei dati dei passeggeri contenuti nella scheda nominativa del passeggero (PNR).

Il GEPD si è inoltre attivato in altre aree, come il settore fiscale e doganale (comprese la cooperazione amministrativa in campo fiscale e la cooperazione

internazionale in campo doganale), gli scambi di dati su larga scala nel contesto del sistema d'informazione del mercato interno, l'utilizzo di scanner di sicurezza negli aeroporti e vari procedimenti giudiziari sul rapporto tra accesso del pubblico e protezione dei dati.

Cooperazione

La principale piattaforma per la cooperazione tra le autorità di protezione dei dati in Europa è il **gruppo di lavoro Articolo 29 per la protezione dei dati**. Il GEPD partecipa alle attività del gruppo, che svolge un ruolo importante nell'applicazione uniforme della direttiva sulla protezione dei dati.

Il GEPD e il gruppo di lavoro Articolo 29 hanno lavorato insieme in buona sinergia su una serie di temi, con particolare riguardo all'applicazione della direttiva sulla protezione dei dati e all'interpretazione di alcune delle sue disposizioni più rilevanti. Il GEPD ha contribuito attivamente in numerose aree, ad esempio con i pareri sui concetti di "responsabile del trattamento" e "incaricato del trattamento", sul principio di responsabilità e sulla normativa applicabile.

Il GEPD ha partecipato anche alle riunioni e attività del gruppo di lavoro Polizia e giustizia, che ha funzioni consultive e si occupa delle questioni che rientrano nell'ex terzo pilastro.

Una delle funzioni di cooperazione più importanti del GEPD comprende l'**Eurodac**, dove le responsabilità del controllo sono condivise con le autorità nazionali di protezione dei dati. Nel 2010 il gruppo di coordinamento del controllo di Eurodac, composto dalle autorità nazionali di protezione dei dati e dal GEPD, si è riunito tre volte a Bruxelles, nei mesi di marzo, ottobre e dicembre, e ha cominciato a lavorare alla preparazione dell'audit completo della sicurezza che sarà eseguito dalle autorità di protezione dei dati sia a livello nazionale sia a livello centrale (UE). Una nuova ispezione coordinata è stata avviata alla fine del 2010; i risultati sono attesi nel 2011.

In merito al controllo del **sistema d'informazione doganale (SID)**, nel 2010 il GEPD ha convocato due riunioni del gruppo di coordinamento del controllo del SID. Alle riunioni hanno partecipato rappresentanti delle autorità nazionali di protezione dei dati nonché rappresentanti dell'autorità comune di controllo in materia doganale e del segretariato della protezione dei dati. Nella riunione di dicembre il gruppo ha adottato un regolamento per disciplinare il suo lavoro futuro riguardo al SID, e ha

esaminato possibili azioni da intraprendere nel periodo 2011-2012 per garantire un controllo generale della protezione dei dati del sistema.

Il GEPD ha continuato a collaborare strettamente con le autorità costituite al fine di esercitare il **controllo comune sui sistemi informatici comunitari su larga scala**.

La cooperazione all'interno di **altri forum internazionali** ha continuato a essere oggetto di attenzione, in particolare le conferenze europea ed internazionale dei commissari responsabili della protezione dei dati e della vita privata, svoltesi rispettivamente a Praga e a Gerusalemme.

In collaborazione con l'Università europea di Firenze, il GEPD ha inoltre organizzato un seminario su **"Protezione dei dati nelle organizzazioni internazionali"**, nel quale sono state affrontate numerose sfide

con cui le organizzazioni internazionali sono confrontate quando cercano di assicurare un buon livello di protezione dei dati in contesti talvolta difficili e privi di una chiara base giuridica.

1.3. Risultati del 2010

Nel 2009 erano stati fissati gli obiettivi principali riportati di seguito; la maggior parte di essi sono stati conseguiti del tutto o in parte.

- **Sostegno alla rete dei responsabili della protezione dei dati**

Il GEPD ha continuato a sostenere con vigore i responsabili della protezione dei dati e ha incoraggiato lo scambio di conoscenze e buone pratiche. All'interno della loro rete, gli RPD hanno elaborato il documento "Standard professionali per i responsabili

Alcune cifre chiave del GEPD nel 2010

→ **55 pareri adottati su controlli preventivi**, riguardanti in particolare dati sanitari, valutazione del personale, assunzioni, gestione del tempo, indagini di sicurezza, registrazioni telefoniche, strumenti di misurazione delle prestazioni

→ **94 reclami ricevuti, di cui 25 giudicati ammissibili**

La maggior parte delle presunte irregolarità riguardava violazioni della segretezza dei dati, raccolte eccessive di dati o uso illegale dei dati da parte del responsabile

• **10 casi risolti** nei quali il GEPD non ha riscontrato violazioni delle norme sulla protezione dei dati

• **11 casi dichiarati non conformi** alle norme sulla protezione dei dati

→ **35 consultazioni su misure amministrative**: è stata fornita consulenza su una vasta gamma di aspetti legali correlati al trattamento dei dati personali da parte delle istituzioni e degli organismi dell'UE

→ **1 ispezione in loco eseguita**

→ **2 orientamenti pubblicati** su indagini amministrative e procedimenti disciplinari e videosorveglianza

→ **19 pareri legislativi emessi** su iniziative riguardanti lo spazio di libertà, sicurezza e giustizia, gli sviluppi tecnologici, la cooperazione internazionale e i trasferimenti di dati, nonché il settore fiscale e quello doganale

→ **7 serie di osservazioni formali** riguardanti, tra l'altro, la revisione del regolamento Frontex, l'apertura di Internet e la neutralità della rete, il sistema d'informazione del mercato interno, gli scanner di sicurezza e gli accordi internazionali sullo scambio di dati

→ **3 riunioni del gruppo di coordinamento del controllo** nelle quali sono stati decisi una nuova ispezione coordinata e i preparativi per un audit completo della sicurezza

→ **12 nuovi funzionari assunti**

della protezione dei dati delle istituzioni e degli organismi dell'UE che operano in conformità del regolamento (CE) n. 45/2001", ultimato nell'ottobre 2010. Il GEPD ha inviato una lettera ai direttori di tutte le istituzioni e agenzie in cui esprime la propria approvazione degli standard e sottolinea l'importanza del ruolo degli RPD ai fini della conformità alle norme sulla protezione dei dati previste dal regolamento.

- **Ruolo del controllo preventivo**

Il GEPD ha quasi concluso il controllo preventivo delle operazioni di trattamento in corso per la maggior parte delle istituzioni e degli organismi di lunga data e ha ulteriormente ribadito l'importanza di dare seguito alle raccomandazioni. Quest'anno sono stati chiusi 137 casi. Un'attenzione speciale è stata riservata al controllo preventivo di operazioni comuni di trattamento dei dati; questi casi sono stati risolti con pareri congiunti.

- **Orientamento orizzontale**

Per contribuire a garantire la conformità delle istituzioni e degli organismi e per uniformare le procedure di controllo preventivo, il GEPD ha pubblicato orientamenti sulle indagini amministrative e sulle procedure disciplinari e sulla videosorveglianza.

- **Politica d'ispezione**

Nel 2010 il GEPD ha proseguito il follow-up di ispezioni precedenti e ha compiuto un'ispezione presso il Centro comune di ricerca della Commissione a Ispra. Nel dicembre 2010 ha reso nota una politica generale per il controllo dei reclami e l'applicazione delle norme sulla protezione dei dati nelle istituzioni e negli organismi.

- **Portata della consultazione**

Il GEPD ha emesso un numero record di pareri – 19 – e sette serie di osservazioni formali concernenti proposte di nuove disposizioni legislative sulla base di un inventario sistematico dei temi e delle priorità pertinenti, e ne ha garantito un seguito adeguato. Tutti i pareri e le osservazioni sono disponibili sul sito, insieme con l'inventario. Un'attenzione particolare è stata riservata al piano d'azione per l'attuazione del programma di Stoccolma.

- **Revisione del quadro giuridico**

In alcune occasioni, utilizzando strumenti diversi, il GEPD ha sollecitato un approccio ambizioso alla

creazione di un quadro moderno e complessivo della protezione dei dati, che copra tutte le aree delle politiche comunitarie, assicuri nei fatti una protezione efficace e possa garantire la certezza del diritto per molti anni. Adesso le pertinenti opinioni del GEPD sono contenute anche in un parere emesso nel gennaio 2011.

- **Agenda digitale**

Il GEPD ha concentrato le proprie attività nell'area della consultazione sulle sfide principali per un'efficace protezione dei dati personali. In tale contesto, è necessario garantire un equilibrio adeguato tra l'esigenza di sicurezza e la protezione dei dati, occuparsi dei progressi tecnologici e affrontare gli effetti dei flussi mondiali di dati. Il GEPD ha dedicato particolare attenzione all'agenda digitale della Commissione in un parere adottato nel marzo 2010, nel quale viene ulteriormente sviluppato il principio di tutela della vita privata fin dalla progettazione.

- **Attività d'informazione**

Il GEPD ha continuato a migliorare la qualità e l'efficacia delle attività di comunicazione e degli strumenti d'informazione. Un importante progresso a tale riguardo è stata l'introduzione del tedesco come terza lingua, oltre all'inglese e al francese, nelle attività di comunicazione e nel servizio stampa.

- **Organizzazione interna**

Si è proceduto a una riorganizzazione del segretariato del GEPD per chiarire meglio le responsabilità e garantire uno svolgimento più efficiente ed efficace dei diversi ruoli e compiti. Nella nuova struttura organizzativa, al direttore spetta il compito di garantire l'attuazione delle politiche e il coordinamento orizzontale delle attività svolte in cinque settori diversi. Il nuovo schema organizzativo è disponibile sul sito.

- **Gestione delle risorse**

Durante il 2010 si è registrato un considerevole aumento (pari a un terzo) del numero dei dipendenti del GEPD. A seguito della riorganizzazione interna si è reso necessario un rinnovato impegno sotto il profilo della programmazione, delle procedure interne e dell'esecuzione del bilancio. Un'attenzione speciale è stata riservata all'esigenza di maggiori spazi di lavoro e all'elaborazione di un sistema di gestione dei casi (CMS).

2

CONTROLLO E APPLICAZIONE DELLA LEGGE

2.1. Introduzione

Il compito del GEPD nella sua veste di autorità indipendente di controllo è quello di monitorare il trattamento dei dati personali da parte delle istituzioni e degli organismi dell'UE (tranne la Corte di giustizia nell'esercizio delle sue funzioni giudiziarie). Il regolamento (CE) n. 45/2001 (in appresso "il regolamento") descrive e conferisce diversi poteri e funzioni che consentono al GEPD di svolgere il proprio compito.

Il trattato di Lisbona segna un cambiamento nel quadro giuridico della protezione dei dati all'interno dell'amministrazione comunitaria con l'introduzione dell'articolo 16 del trattato sul funzionamento dell'Unione europea, che sostituisce l'articolo 286 del trattato CE. Per effetto dell'abolizione della struttura a pilastri, i compiti di controllo del GEPD coprono ora, in linea di principio, tutte le istituzioni e tutti gli organismi dell'UE, anche in aree completamente estranee al campo di applicazione di ciò che era il "diritto comunitario" ⁽⁵⁾, ove non diversamente previsto in maniera specifica da altri atti comunitari. Le implicazioni precise di queste modifiche delle attività di controllo del GEPD sono tuttora oggetto di analisi e potrebbero richiedere ulteriori approfondimenti.

Anche nel corso del 2010 il controllo preventivo delle operazioni di trattamento è stato un aspetto importante dell'attività di controllo (cfr. sezione 2.3);

un'enfasi particolare è stata data al seguito delle raccomandazioni formulate nei pareri del GEPD. Il Garante ha inoltre elaborato altre forme di controllo, quali la gestione dei reclami, le ispezioni, la consulenza su misure amministrative e la stesura di orientamenti tematici. Il controllo da parte del GEPD è un'attività specifica che necessita di una stretta collaborazione con le autorità nazionali di protezione dei dati (cfr. sezione 4.2).

Il GEPD ha altresì adottato una politica per i reclami e l'applicazione della legge, a testimonianza di un maggiore impegno nell'applicazione del regolamento.

2.2. Responsabili della protezione dei dati

Un elemento interessante nel panorama della protezione dei dati delle istituzioni comunitarie è l'obbligo di nominare un responsabile della protezione dei dati (RPD), ai sensi dell'articolo 24, paragrafo 1, del regolamento. Alcune istituzioni hanno affiancato all'RPD un assistente o un responsabile aggiunto. La Commissione ha nominato un responsabile della protezione dei dati per l'Ufficio europeo per la lotta antifrode (OLAF, una direzione generale della Commissione). Alcune istituzioni hanno nominato anche coordinatori della protezione dei dati, al fine di coordinare tutti gli aspetti della protezione dei dati all'interno di una data direzione o unità.

Nel 2010 sono stati istituiti due nuovi responsabili della protezione dei dati in nuove agenzie o imprese comuni; il numero totale degli RPD è così salito a 47.

⁽⁵⁾ Cfr. articolo 3, paragrafo 1, del regolamento (CE) n. 45/2001, che adesso è meno rilevante rispetto a prima del 1o dicembre 2009.

Per alcuni anni i responsabili della protezione dei dati si sono riuniti periodicamente per condividere le esperienze comuni e discutere questioni orizzontali. Questa rete informale si è rivelata proficua sotto il profilo della collaborazione ed è proseguita per tutto il 2010.

È stato costituito un “quartetto di RPD”, formato da quattro responsabili (del Consiglio, del Parlamento europeo, della Commissione europea e del Centro di traduzione degli organismi dell’Unione europea), con funzioni di coordinamento della rete dei responsabili della protezione dei dati. Il GEPD ha collaborato strettamente con il quartetto.

Il GEPD ha partecipato alle riunioni dei responsabili della protezione dei dati svoltesi nel marzo 2010 presso la Banca europea per gli investimenti, a Lussemburgo, e nell’ottobre 2010 presso l’Agenzia europea per i medicinali, a Londra, e ha colto l’occasione per aggiornare i responsabili sul proprio lavoro, fornire una panoramica degli sviluppi recenti nel campo della protezione dei dati nell’Unione europea e trattare questioni di comune interesse.

Più nello specifico, il GEPD ha utilizzato questo forum per illustrare e discutere la procedura dei controlli preventivi, relazionare sui progressi compiuti riguardo alle notifiche di controlli preventivi, aggiornare gli RPD sulle discussioni con i comitati interistituzionali, illustrare la sua nuova struttura e presentare i suoi orientamenti tematici. Il GEPD ha

inoltre informato i responsabili della protezione dei dati dell’adozione della politica per i reclami e l’applicazione della legge. Il forum è servito anche per condividere iniziative in occasione della Giornata europea della protezione dei dati (28 gennaio).

All’interno della loro rete, i responsabili della protezione dei dati hanno stilato un documento dal titolo “Standard professionali per i responsabili della protezione dei dati delle istituzioni e degli organismi dell’UE che operano in conformità del regolamento (CE) n. 45/2001”, che è stato ultimato nella riunione del 14 ottobre 2010 della rete degli RPD. Il GEPD ha inviato ai direttori di tutte le istituzioni e agenzie una lettera in cui esprime la propria approvazione degli standard e sottolinea l’importanza del ruolo degli RPD ai fini della conformità alle norme sulla protezione dei dati previste dal regolamento. Il GEPD intende richiamarsi a questo documento, ove del caso, nello svolgimento delle proprie funzioni di controllo delle istituzioni e degli organismi.



I responsabili della protezione dei dati durante la riunione a Bruxelles (marzo 2010).

2.3. Controlli preventivi

2.3.1. Base giuridica

Il regolamento (CE) n. 45/2001 prevede che tutte le operazioni di trattamento dei dati tali da comportare rischi specifici per i diritti e le libertà delle persone interessate, a causa della loro natura, portata o delle loro finalità, siano sottoposte a controllo preventivo da parte del GEPD (articolo 27, paragrafo 1).

L'articolo 27, paragrafo 2, del regolamento contiene un elenco non esaustivo delle operazioni di trattamento che possono comportare tali rischi. Per l'interpretazione di questa norma si sono continuati ad

applicare i criteri definiti negli anni scorsi ⁽⁶⁾, sia per decidere che una notifica da parte di un responsabile della protezione dei dati non era soggetta a controllo preventivo, sia per fornire consulenza sulla necessità di un controllo preventivo (cfr. anche sezione 2.3.4).

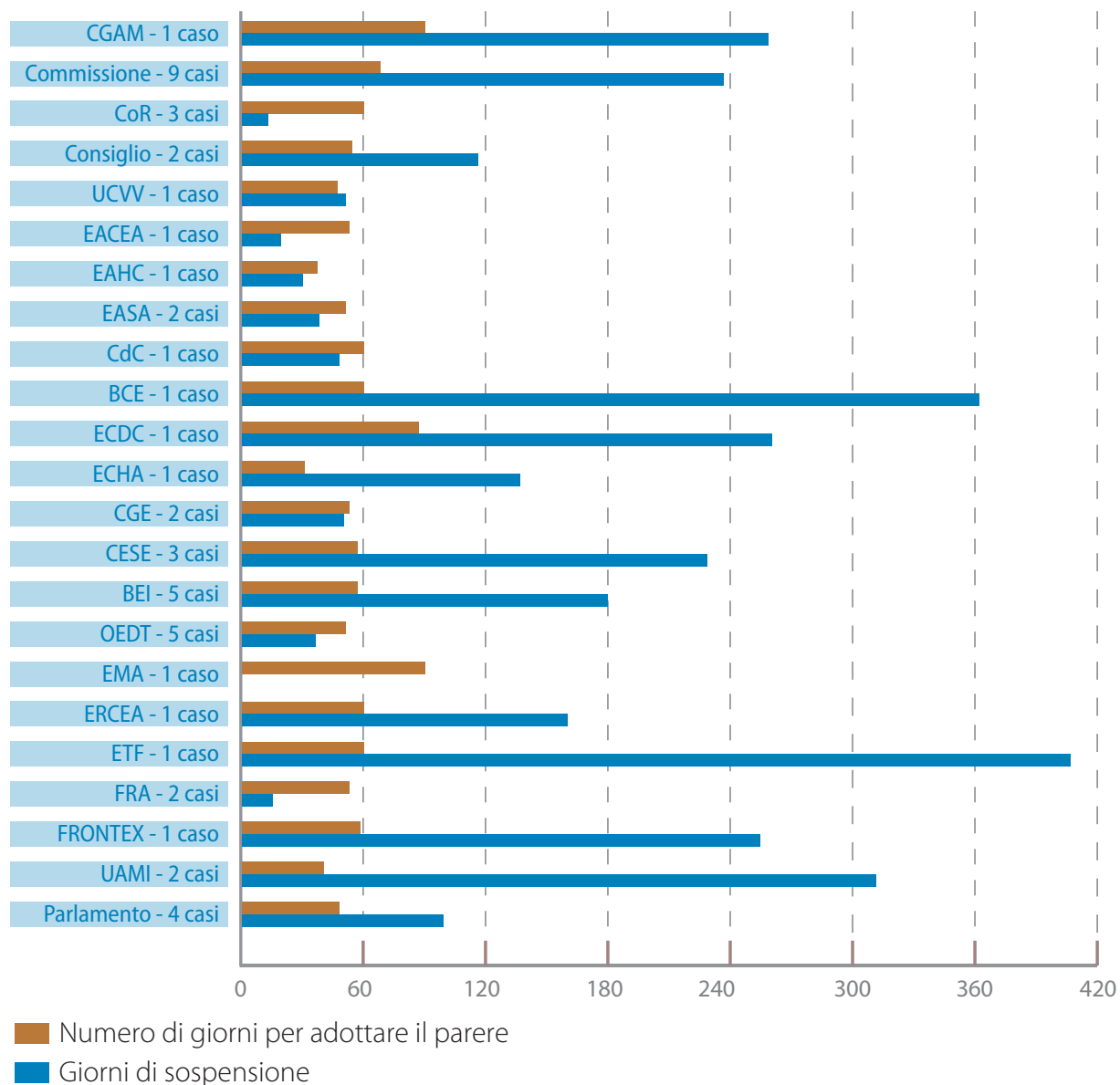
2.3.2. Procedura

Notifica

I controlli preventivi devono essere effettuati dal GEPD previa ricezione di una notifica da parte di un responsabile della protezione dei dati. Qualora questi nutra dubbi sulla necessità di sottoporre

⁽⁶⁾ Cfr. relazione annuale 2005, sezione 2.3.1.

Scadenze medie per istituzione/agenzia



un'operazione di trattamento a controllo preventivo, può consultare il GEPD (cfr. sezione 2.3.4).

I controlli preventivi riguardano operazioni non ancora in corso, ma anche trattamenti iniziati prima del 17 gennaio 2004 (ossia la data di istituzione del primo Garante europeo della protezione dei dati e del primo Garante aggiunto) o prima dell'entrata in vigore del regolamento (controlli preventivi ex post). In tali circostanze, un controllo ai sensi dell'articolo 27 non può essere considerato "preventivo" nel senso stretto del termine, bensì deve essere gestito secondo modalità ex post.

Durata, sospensione ed estensione

Il GEPD deve fornire il proprio parere entro due mesi dalla ricezione della notifica (7). Qualora richieda informazioni aggiuntive, il periodo di due mesi viene di solito sospeso fino a quando il GEPD riceve le informazioni richieste. Il periodo di sospensione comprende il tempo concesso al responsabile della protezione dei dati per formulare le proprie osservazioni e, ove necessario, per fornire ulteriori informazioni sulla bozza finale. In casi complessi, il GEPD può anche prorogare il periodo iniziale di altri due mesi. Se al termine del periodo di due mesi o della proroga non è stata presa alcuna decisione, il parere del GEPD è considerato favorevole. Ad oggi non ci sono stati casi del genere, ossia di tacito parere favorevole.

(7) Per i casi ex post pervenuti entro il 1o settembre 2010, il mese di agosto non è stato considerato né per le istituzioni e gli organismi né per il GEPD.

Registro

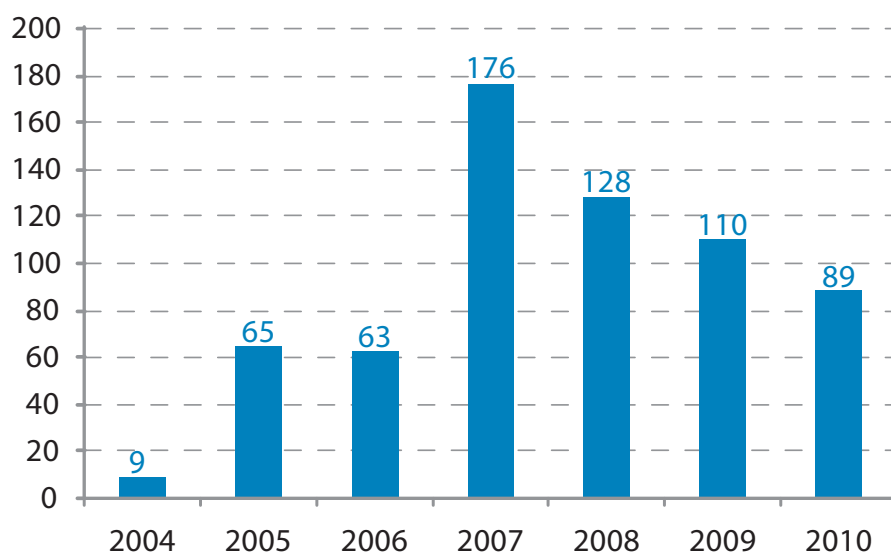
Nel 2010 il GEPD ha ricevuto 89 notifiche di controllo preventivo. Questa cifra rivela un leggero calo rispetto al 2009, perché il GEPD sta smaltendo gli arretrati dei controlli preventivi ex post.

Il regolamento stabilisce che il GEPD debba tenere un registro di tutte le operazioni di trattamento che gli sono state notificate a fini di controllo preventivo (articolo 27, paragrafo 5). Il registro deve contenere le informazioni di cui all'articolo 25 ed essere aperto alla consultazione pubblica. Nell'interesse della trasparenza, tutte le informazioni sono contenute nel registro pubblico disponibile sul sito del GEPD (tranne le misure di sicurezza che non sono riportate nel registro).

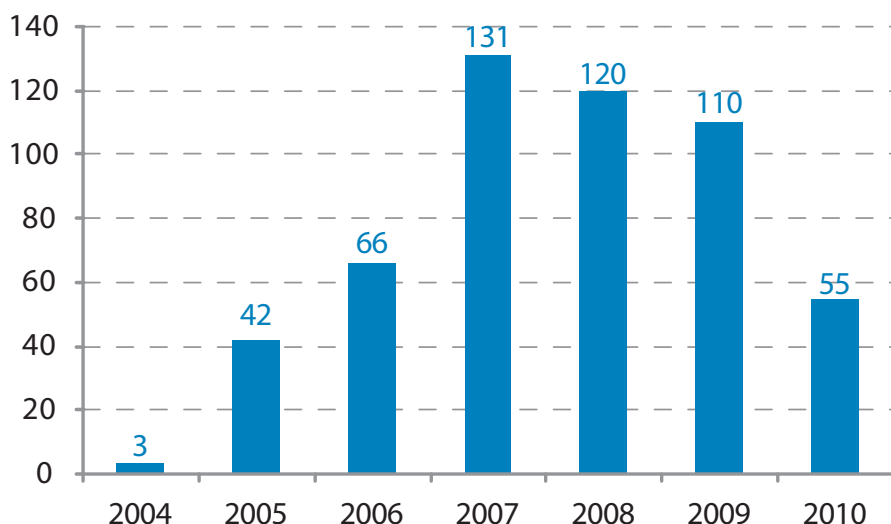
Pareri

La posizione finale del GEPD viene redatta in forma di un parere notificato al responsabile dell'operazione di trattamento e al responsabile della protezione dei dati dell'istituzione o dell'organismo interessato (articolo 27, paragrafo 4). Nel 2010 il GEPD ha adottato **55 pareri di controllo preventivo** (cfr. più sopra il grafico "Pareri di controllo preventivo del GEPD per anno") e **8 controlli non preventivi** (cfr. sezione 2.3.5). Pur trattandosi di un calo rispetto agli anni precedenti, vale la pena rilevare che, a seguito degli orientamenti sulla videosorveglianza e sulle assunzioni, il GEPD si è occupato di un numero significativo di casi mediante pareri congiunti, affrontandoli quindi in modo più efficiente.

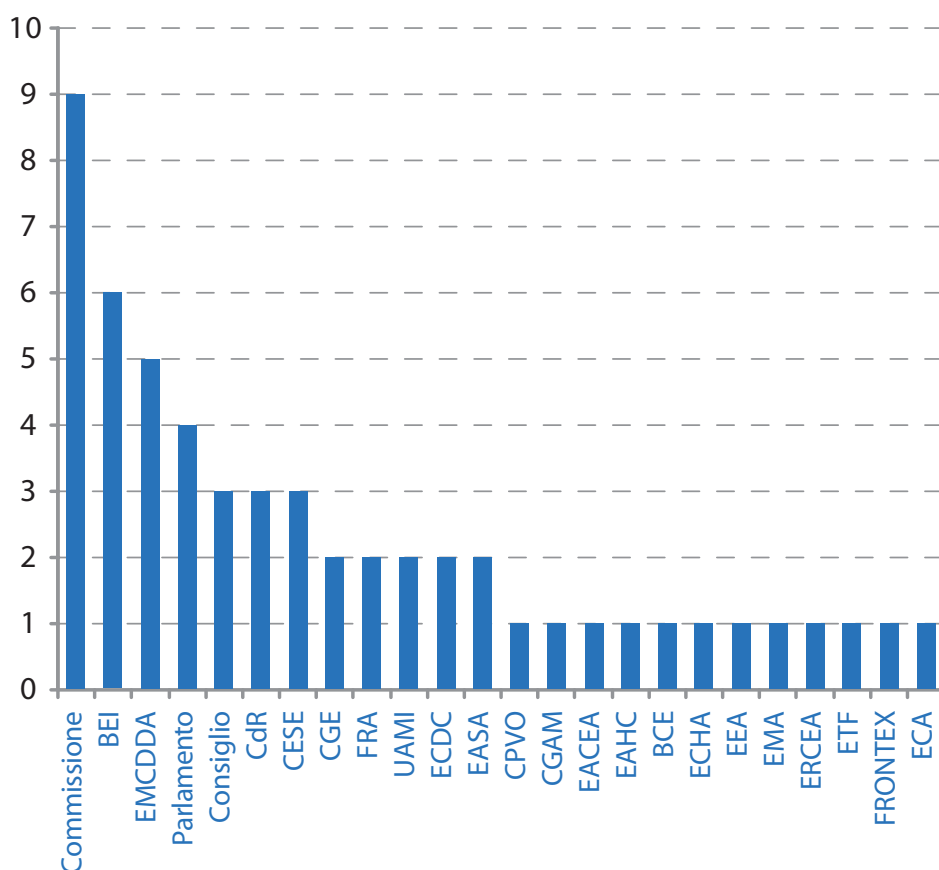
Notifiche al GEPD



Pareri di controllo preventivo del GEPD per anno



Pareri di controllo preventivo del GEPD per istituzione nel 2010



La **gran parte di questi pareri** sono destinati alle **istituzioni più grandi**, con nove pareri di controllo preventivo (e tre di controllo non preventivo) riguardanti le operazioni di trattamento presso la Commissione europea, quattro presso il Parlamento europeo e tre presso il Consiglio (cfr. più sopra il grafico “Pareri del GEPD per istituzione”). Anche le agenzie hanno continuato

a notificare attività operative centrali e procedure amministrative standard in conformità delle pertinenti procedure stabilite dal GEPD (cfr. sezione 2.3.2).

I pareri contengono una descrizione dei procedimenti, una sintesi dei fatti e un’analisi giuridica volta ad accertare se le operazioni di trattamento sono

conformi alle rilevanti disposizioni del regolamento. Ove necessario, vengono formulate raccomandazioni al responsabile, al fine di assicurare la conformità al regolamento. Nelle sue conclusioni il GEPD scrive solitamente che il trattamento non sembra configurare alcuna violazione delle disposizioni del regolamento, purché si tenga conto delle sue raccomandazioni.

Una volta emesso, il parere del GEPD è reso pubblico. Tutti i pareri sono disponibili sul sito del GEPD, insieme con una sintesi del caso esaminato.

Un manuale di casistica assicura che tutto il gruppo lavori sulle stesse basi e che i pareri del GEPD siano adottati dopo un'analisi completa di tutte le informazioni rilevanti. Il manuale fornisce un modello per la stesura dei pareri che è fondato sull'esperienza pratica acquisita e viene aggiornato costantemente. Si utilizza un sistema di flusso di lavoro per garantire il seguito di tutte le raccomandazioni riguardanti un caso specifico e, ove pertinente, il rispetto di tutte le decisioni di applicazione delle norme (cfr. sezione 2.3.6).

Procedura per i controlli preventivi ex post nelle agenzie

Nell'ottobre 2008 il GEPD ha lanciato una nuova procedura per i controlli preventivi ex post nelle agenzie comunitarie. Poiché le procedure standard sono uguali nella maggior parte delle agenzie dell'UE e si basano su decisioni della Commissione, l'intento è quello di raccogliere le notifiche su argomenti simili e o adottare un parere collettivo (valido per più agenzie) o compiere un "mini controllo preventivo" che tenga conto soltanto delle esigenze specifiche

di un'agenzia. Per aiutare le agenzie a completare le loro notifiche, il GEPD presenta un riassunto dei punti e delle conclusioni principali sull'argomento, alla luce dei pareri sui controlli preventivi emessi in precedenza in forma di orientamenti tematici (cfr. sezione 2.7. Orientamenti tematici).

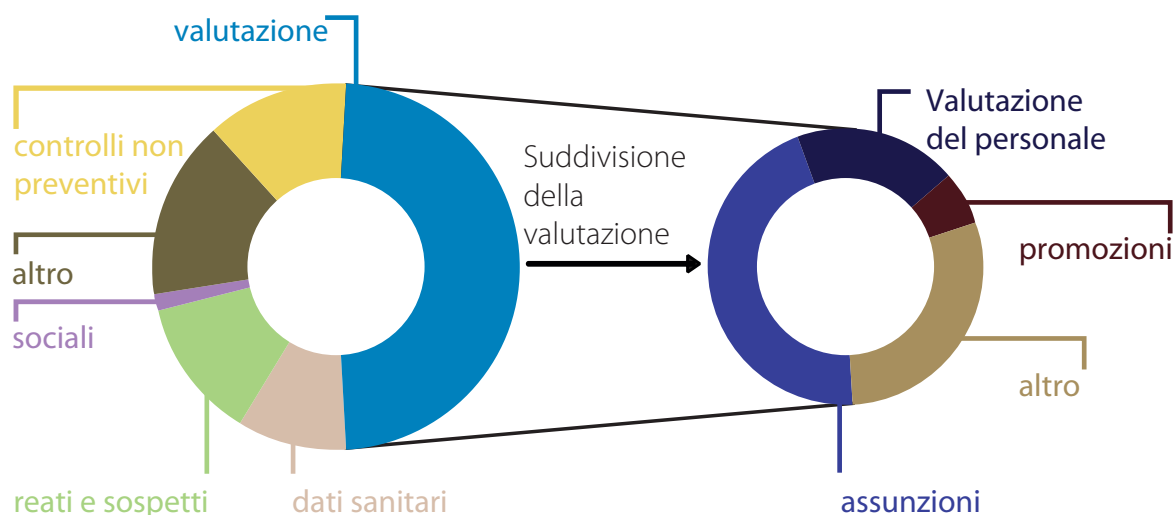
Il primo argomento affrontato è stato quello delle **assunzioni**, sul quale il GEPD ha emesso nel maggio 2009 un parere orizzontale che riguarda notifiche provenienti da 12 agenzie. Alla fine di settembre 2009 alle agenzie è stata inviata una seconda serie di orientamenti, concernenti il **trattamento dei dati sanitari**. Al momento della stesura della presente relazione, il GEPD aveva inviato un parere orizzontale alle 19 agenzie chiedendo loro di formulare osservazioni, e spera di poterlo adottare all'inizio del 2011. Nell'aprile 2010 il GEPD ha pubblicato orientamenti sul trattamento dei dati personali nelle **indagini amministrative e nei procedimenti disciplinari** avviati dalle istituzioni e dagli organismi comunitari. Il GEPD sta ricevendo dalle agenzie notifiche relative a questo settore e intende adottare un parere congiunto nei primi sei mesi del 2011.

2.3.3. Questioni principali trattate nell'ambito dei controlli preventivi

2.3.3.1. Sistema di allarme rapido e di reazione – Commissione europea

Il sistema di allarme rapido e di reazione (EWRS) è uno strumento di comunicazione utilizzato dalla Commissione, dal Centro europeo per la

Pareri 2010 per categoria



prevenzione e il controllo delle malattie (ECDC) e dagli Stati membri dell'Unione europea per scambiarsi informazioni sulla prevenzione di malattie trasmissibili (come tubercolosi, morbillo, ARS, H1N1 e altre) allo scopo di facilitare le azioni transfrontaliere. Una caratteristica del sistema è l'"**individuazione del contatto**", una procedura che serve a identificare e rintracciare le persone che possono essere venute a contatto con un soggetto infetto. Dopo aver rintracciato queste persone, si può fare una diagnosi e curarle. L'individuazione del contatto è anche nell'interesse della salute pubblica generale perché riduce o previene l'ulteriore diffusione di una malattia.

Nel suo parere (fascicolo 2009-0137) il GEPD si è concentrato sulla necessità di **stabilire con chiarezza i ruoli, i compiti e le responsabilità** delle parti interessate per quanto riguarda la gestione e l'utilizzo del sistema, con particolare attenzione al ruolo della Commissione e dell'ECDC. I controllori e gli incaricati del trattamento dei dati devono essere designati in modo chiaro e corrispondente ai loro ruoli effettivi; lo stesso vale per lo status giuridico delle organizzazioni interessate.

Si devono specificare con esattezza le responsabilità delle parti coinvolte e i modi in cui gli interessati possono esercitare i loro diritti. In una prospettiva di breve periodo, è stato consigliato che il sistema di allarme rapido e di reazione adotti una serie di orientamenti per la protezione dei dati. Anche la Commissione è stata sollecitata a rivedere il quadro giuridico, per garantire una base giuridica più sicura e una chiara attribuzione delle responsabilità.

Inoltre, il GEPD ha sottolineato l'esigenza di dare attuazione al principio della "**tutela della vita privata fin dalla progettazione**" e di integrare la protezione dei dati nella formazione fornita agli utenti. Appare opportuna l'istituzione di un meccanismo chiaro per l'esercizio del **diritto di accesso** da parte degli interessati. Infine, per garantire coerenza e trasparenza, l'operatore del sistema dovrebbe rendere disponibili sul proprio sito informazioni generali e facilmente comprensibili per gli interessati, da integrare con note informative fornite dai punti di contatto degli Stati membri in conformità delle norme nazionali sulla protezione dei dati.



L'EWRS è uno strumento di comunicazione per lo scambio di informazioni sulle malattie trasmissibili.

2.3.3.2. Sistema europeo di sorveglianza ("TESSy") – Centro europeo per la prevenzione e il controllo delle malattie

Il 3 settembre 2010 il GEPD ha emesso un parere di controllo preventivo (fascicolo 2009-0474) sugli aspetti correlati alla protezione dei dati del sistema TESSy. TESSy è uno strumento di comunicazione del Centro europeo per la prevenzione e il controllo delle malattie che mira a garantire uno scambio rapido ed efficace dei dati sulla sorveglianza epidemiologica tra gli Stati membri dell'Unione europea.

Nel parere si spiega come i **dati statistici** continuino a essere considerati "dati personali" e in quanto tali siano soggetti al regolamento qualora le persone interessate possano essere identificate, almeno indirettamente. Il fatto che si sia fatto ricorso a determinate "tecniche per rendere anonimi" i dati non significa necessariamente che essi siano considerati "dati resi anonimi" nel significato che ne dà il considerando 8 del regolamento, e quindi cessino di essere considerati "dati personali".

Il GEPD ha ribadito molte delle raccomandazioni espresse nel suo parere sul sistema di allarme rapido e di reazione (cfr. sopra) e ha aggiunto che sarebbe opportuno adottare quanto prima possibile una specifica politica di sicurezza, per contribuire a garantire la sicurezza del sistema europeo di sorveglianza.

2.3.3.3. Piano congiunto per l'assicurazione contro le malattie

Il Comitato di gestione del regime comune di assicurazione malattia (CGAM) è responsabile della gestione del regime comune di assicurazione malattia. Il Comitato è composto dai rappresentanti del personale designati dai comitati del personale di ciascuna istituzione nonché dai rappresentanti delle amministrazioni. Si occupa di tutte le modifiche delle norme e dei reclami presentati dai membri; inoltre, emette pareri e raccomandazioni e avanza proposte sull'operatività del piano.

Il GEPD si è incontrato con il Comitato nel novembre 2008 per discutere questioni attinenti alla protezione dei dati in relazione ai documenti gestiti dal Comitato stesso. Poiché i reclami presentati dai membri

affiliati contengono spesso dati sensibili, si è deciso che il Comitato avrebbe inviato una notifica al GEPD.

Detta notifica ha portato alla stesura di un parere (fascicolo 2009-0070), emesso l'8 gennaio 2010, nel quale il GEPD ha formulato raccomandazioni concernenti in particolare la **trasmissione di dati personali** al CGAM, il **periodo di conservazione** su CIRCA (un'applicazione basata sul web per gruppi di lavoro che utilizzano dati condivisi) e l'adozione di un'**adeguata politica di sicurezza** entro sei mesi dall'adozione del parere.

2.3.3.4. Ispezioni di sicurezza – Commissione europea (DG Centro comune di ricerca di Ispra)

Il 6 settembre 2010 (fascicolo 2009-0682) il GEPD ha emesso un parere di controllo preventivo riguardante le ispezioni di sicurezza presso il Centro comune di ricerca della Commissione europea a Ispra. Sono state esaminate le operazioni di trattamento dei dati compiute al fine di mantenere e migliorare gli standard di sicurezza applicabili.

Il GEPD ha riconosciuto che la "procedura in caso d'infortunio" comporta il trattamento di dati sanitari da parte di numerosi soggetti, allo scopo di prevenire e ridurre al minimo le conseguenze di incidenti alla sicurezza presso il Centro di Ispra.

Il GEPD ha formulato raccomandazioni al fine di **garantire il rispetto del principio di "limitazione del campo di applicazione" in caso di trasferimento di dati** e la **conformità ai principi della qualità dei dati** applicabili alla conservazione e al trattamento successivo dei dati personali trattati in tale contesto. È stata inoltre suggerita una revisione in questo senso della dichiarazione attualmente in uso sul rispetto della vita privata.

2.3.3.5. Inventario per il testo di autovalutazione BELBIN – Scuola europea di amministrazione

Lo scopo del trattamento è quello di permettere ai partecipanti ai corsi di formazione della Scuola europea di amministrazione (EAS) di avere un riscontro in forma di relazione sul ruolo preferito all'interno di un gruppo. Questo dato non può essere utilizzato per alcun tipo di valutazione della persona interessata. Nel parere del 15 marzo 2010 (fascicolo 2009-0377) il GEPD si è concentrato su due aspetti:

- **il rapporto tra il responsabile, l'incaricato del trattamento e il subappaltatore:** anche se l'EAS non ha accesso ai dati trattati dal subappaltatore, questi deve agire in conformità delle istruzioni date dall'EAS all'appaltatore. L'EAS è il responsabile di questa attività di trattamento perché è lei a stabilire le finalità e i mezzi da usare (lo strumento basato sul web). I tre appaltatori responsabili della fornitura dei corsi di formazione e il subappaltatore responsabile dello strumento basato sul web sono considerati incaricati del trattamento dei dati personali che agiscono su incarico dell'EAS. Il subappaltatore non è autorizzato a compiere alcuna attività di trattamento successivo che ecceda quanto stabilito dall'EAS e quanto specificato nel contratto tra il subappaltatore e l'appaltatore, conformemente al contratto tra l'EAS e quest'ultimo;
- **il carattere di anonimità dei dati:** la relazione consegnata ai partecipanti non può essere considerata "anonima" perché il subappaltatore è in grado di collegare le risposte agli interessati, dato che i partecipanti di solito usano un indirizzo di posta elettronica che contiene il loro nome e cognome.

Il GEPD ha formulato raccomandazioni su questi due aspetti, sostenendo in particolare che il contratto dovrebbe prevedere clausole su tutte le caratteristiche obbligatorie, cioè **riservatezza e sicurezza del trattamento** tra l'appaltatore e il subappaltatore.

2.3.3.6. Controllo elettronico – Corte dei conti

La **Corte dei conti** ha definito una procedura per **accedere a unità e messaggi di posta elettronica privati** per poter gestire varie situazioni (ad

esempio, quando un dipendente muore, cessa di lavorare per l'istituzione o è assente) nelle quali le informazioni contenute nelle unità e nei messaggi privati sono necessarie per il funzionamento dell'istituzione. La procedura proposta stabilisce che chi richiede le informazioni debba compilare un modulo standard. La richiesta deve contenere una descrizione dettagliata del o dei motivi che giustificano l'accesso, il o i nomi dei documenti o l'account di posta elettronica e/o l'oggetto dell'informazione. Il modulo va inviato al funzionario responsabile della sicurezza delle informazioni o, in sua assenza, al funzionario responsabile della sicurezza fisica.



Presso la Corte dei conti è stata elaborata una procedura per accedere a unità e messaggi di posta elettronica privati.

Originariamente la richiesta veniva spedita al GEPD per consultazione, poiché questa procedura **comporta potenzialmente l'accesso a dati riservati** e il GEPD riteneva effettivamente che tale operazione di trattamento presentasse rischi specifici che necessitavano di una notifica di controllo preventivo.

Nel parere del 10 gennaio 2010 (fascicolo 2009-0620) il GEPD ha raccomandato alla Corte dei conti di adottare una **base giuridica specifica** per l'uso e la conservazione dei messaggi di posta elettronica privati e ha fissato **orientamenti chiari per gli utenti** sull'utilizzo delle risorse della rete e dei messaggi di posta elettronica.

2.3.3.7. Detrazioni salariali in caso di sciopero – Banca centrale europea

Ai sensi dell'articolo 1.4 dello statuto del personale della Banca centrale europea (BCE), ai dipendenti è riconosciuto il diritto di sciopero. L'articolo 1.4.5 stabilisce che, a meno che il comitato esecutivo non decida diversamente, la durata complessiva

dello sciopero debba essere detratta dalle somme dovute a titolo di stipendio ai membri del personale che partecipano allo sciopero. Inoltre, l'articolo 1.4.7 stabilisce che "Nessun provvedimento disciplinare può essere adottato nei confronti di un membro del personale che partecipi a uno sciopero, a meno che egli non sia stato incaricato di garantire le predette condizioni minime di servizio e abbia ommesso di farlo al fine di partecipare allo sciopero".

Nella misura in cui la partecipazione a uno sciopero comporta automaticamente una detrazione di stipendio e di altre indennità, il trattamento dei dati personali correlati a tale detrazione è soggetto a controllo preventivo da parte del GEPD perché si tratta di un trattamento volto a privare persone del godimento di un diritto, beneficio o contratto.

Il 28 settembre 2010 il GEPD ha emesso un parere di controllo preventivo (fascicolo 2009-0514) in merito a un'operazione di trattamento dati del genere su descritto e ha formulato raccomandazioni sui **periodi di conservazione** di qualsiasi documentazione conservata nel sistema elettronico di gestione dei documenti e delle registrazioni della BCE, nonché sulle **informazioni** da fornire agli interessati.

2.3.3.8. Indagini su frodi – Banca europea per gli investimenti

La divisione Indagini antifrode della Banca europea per gli investimenti (BEI) indaga su denunce di pratiche illecite ai sensi delle procedure antifrode della BEI. Per poter eseguire tali indagini, la divisione ha pieno accesso a tutte le informazioni, i documenti e i dati pertinenti riguardanti il personale, compresi i dati elettronici conservati all'interno della BEI; non sono tuttavia ammesse intercettazioni di comunicazioni né di conversazioni. Spetta al capodivisione stabilire se un reclamo o un'accusa siano stati provati e sottoporre il caso alle autorità responsabili all'interno e/o all'esterno della BEI, per quanto di loro competenza. Qualora, dopo un'indagine ragionevole, la divisione Indagini antifrode accerti che un reclamo o un'accusa non sono stati provati, documenterà i risultati dell'indagine in una nota relativa al fascicolo e chiuderà il caso.

Il GEPD ha emesso un parere di controllo preventivo (fascicolo 2009-0459) su operazioni di trattamento di dati relative a indagini su frodi e ha raccomandato alla BEI di valutare la **base giuridica** di tali indagini, adottare un **protocollo formale per l'esecuzione di indagini forensi computerizzate**, armonizzare i periodi di conservazione e fornire informazioni agli interessati.



La divisione Indagini antifrode della BEI indaga su denunce di pratiche illecite.

2.3.3.9. Analisi empirica delle correlazioni tra le variabili del sistema di lavoro e il processo decisionale – Ufficio per l'armonizzazione nel mercato interno

Questo controllo preventivo (fascicolo 2010-0468) ha riguardato gli aspetti relativi alla protezione dei dati di un esercizio compiuto dall'Ufficio per l'armonizzazione nel mercato interno (UAMI) dal titolo "Analisi empirica delle correlazioni tra le variabili del sistema di lavoro e il processo decisionale". Lo scopo dell'analisi era di contribuire all'individuazione di profili professionali comparabili e delle migliori pratiche nella gestione delle risorse umane per tali profili. Oltre ai vantaggi pratici per l'UAMI, questo progetto perseguiva anche scopi scientifici perché l'analista che ha compiuto l'indagine intendeva pubblicarne i risultati in una tesi di dottorato (dopo una redazione accurata e rispettosa della vita privata dei partecipanti all'esercizio). Il GEPD ha formulato alcune raccomandazioni riguardanti in particolare la conservazione dei dati, i trasferimenti a terzi e le informazioni agli interessati.

Il GEPD ha raccomandato la cancellazione di tutti i dati personali dai server dell'UAMI alla fine del periodo di conservazione (2011). Ha inoltre consigliato all'analista di tener conto delle legislazioni nazionali vigenti in materia di microdati conservati per potenziali ricerche future o trasferiti a terzi, allo scopo di garantire la conformità agli obblighi di necessità, finalità e riservatezza.

2.3.3.10. La Banca dati centrale sulle esclusioni – Commissione europea

A tutela degli interessi finanziari delle istituzioni e in ottemperanza del regolamento finanziario, la Commissione europea tratta dati contenuti in una banca dati centrale sulle esclusioni. Questi dati possono essere utilizzati solamente al fine di escludere soggetti che rappresentano una minaccia per gli interessi finanziari europei da qualsiasi procedura di appalto o prestito finanziata con fondi comunitari o del Fondo di sviluppo europeo.

Il GEPD ha condotto un'analisi (fascicolo 2009-0681) alla quale l'istituzione interessata ha collaborato pienamente sin dall'inizio.

Il GEPD ha concluso che non c'era motivo di ritenere che fossero state violate le disposizioni del regolamento sulla protezione dei dati. Ha nondimeno formulato alcune raccomandazioni sulle informazioni preventive che devono essere fornite a candidati, offerenti e richiedenti prestiti negli inviti a presentare proposte e nei bandi di gara.

2.3.3.11. Operazioni di rimpatrio congiunte – Frontex

Il 26 aprile 2010 il GEPD ha adottato un parere (fascicolo 2009-0281) sul trattamento di dati personali da parte di Frontex in merito alla "raccolta di nomi e altri dati pertinenti dei rimpatriati nelle operazioni di rimpatrio congiunte (JRO)". Lo scopo del trattamento di questi dati è di preparare e attuare le operazioni di rimpatrio congiunte con l'aiuto di Frontex in modo tale da consegnare alle compagnie aeree un elenco dei passeggeri e conoscere, tra l'altro, il numero e l'identità dei rimpatriati, i rischi ad essi collegati e i rischi per la sicurezza di dette operazioni, nonché le condizioni di salute dei rimpatriati, al fine di garantire un'adeguata assistenza medica durante le operazioni.

Frontex ha comunicato al GEPD che i dati personali non erano stati ancora trattati per attività operative, ma che un tanto si sarebbe reso necessario in futuro per, primo, adempiere meglio e sviluppare ulteriormente i compiti dell'agenzia nel contesto delle operazioni di rimpatrio congiunte; secondo, aiutare lo Stato membro o il paese associato a Schengen che organizza tali operazioni a compilare e aggiornare gli elenchi dei passeggeri; terzo, avere una costante visione d'insieme di quale Stato membro o paese associato a Schengen che partecipa a tali operazioni abbia (o non abbia) fornito i dati richiesti allo Stato organizzatore; quarto, rendere più efficiente ed efficace l'assistenza fornita da Frontex per l'organizzazione delle operazioni di rimpatrio congiunte.

Il GEPD ha riservato un'attenzione particolare alla base giuridica del trattamento.

Ha riconosciuto che talune operazioni di trattamento dei dati personali possono essere necessarie ai fini di un corretto svolgimento dei compiti dell'agenzia nel contesto delle operazioni di rimpatrio congiunte, delle quali l'agenzia può essere considerata responsabile. Ma, visto il carattere sensibile dei dati e delle attività nei confronti di persone vulnerabili, il GEPD ha ritenuto che l'articolo 9 del regolamento Frontex (cooperazione in materia di rimpatrio) e l'articolo 5, lettera a), del regolamento sulla protezione dei dati possano costituire soltanto una base giuridica provvisoria per l'attività di trattamento, la quale va sottoposta a un'attenta revisione sotto il profilo della necessità di una base giuridica più specifica.

Il GEPD ha chiesto inoltre che Frontex attui le **procedure necessarie a garantire i diritti degli interessati** e adempia l'**obbligo d'informazione** prima dell'inizio del trattamento.

2.3.4. Consultazioni sulla necessità di controlli preventivi

La semplice possibilità della presenza di **dati sensibili** non significa automaticamente che si debba procedere a un controllo preventivo. Tuttavia, il trattamento di dati sensibili concernenti, per esempio, la salute o illeciti penali/civili deve avvenire nel rispetto di adeguate misure di sicurezza, conformemente all'articolo 22 del regolamento.

In caso di dubbio, le istituzioni e gli organismi comunitari possono consultare il GEPD sulla necessità di procedere a un controllo preventivo. Nel corso del 2010 il GEPD ha ricevuto sei richieste di consultazione a tale proposito da responsabili della protezione dei dati.

Tra le questioni prese in esame dal GEPD figuravano le procedure di selezione di funzionari di alto livello, le liste di presenza dei membri delle associazioni partecipanti a eventi presso un'istituzione, le attività di trattamento da parte di un comitato del personale e una politica di formazione del personale.

2.3.5. Notifiche non soggette a controllo preventivo o ritirate

Nel 2010 il GEPD ha accertato, dopo attenta analisi, che otto casi non erano soggetti a controllo

preventivo; su di essi, tuttavia, il GEPD può formulare raccomandazioni. Inoltre, tre notifiche sono state ritirate e una è stata sostituita.

In un caso concernente la formazione (fascicolo 2010-0638), informazioni aggiuntive fornite dall'Autorità europea per la sicurezza alimentare (EFSA) nel contesto della notifica hanno permesso di chiarire che i dati raccolti erano perlopiù dati statistici e avevano come unica finalità quella di garantire la qualità della politica di formazione dell'EFSA. Sebbene sia ammesso includere dati sulla valutazione della formazione, la relazione prodotta non aveva lo scopo di valutare singoli formatori. Sulla base di questa informazione, il GEPD ha ritenuto che la notifica in questione non fosse soggetta a controllo preventivo.

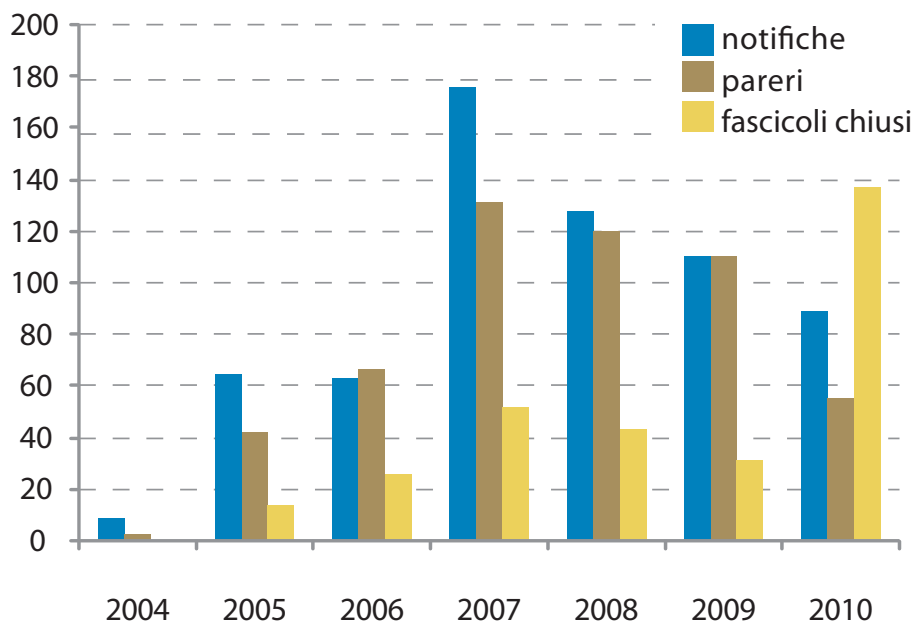
2.3.6. Seguito dato ai pareri di controllo preventivo

*Di solito, un parere del GEPD sul controllo preventivo si conclude con la constatazione che l'operazione di trattamento dei dati non viola il regolamento purché siano attuate determinate **raccomandazioni**. Vengono formulate raccomandazioni anche quando si esamina un caso per decidere sulla necessità di un controllo preventivo e risulta necessario apportare misure correttive a taluni aspetti critici. Qualora il responsabile del trattamento dei dati non si conformi a tali raccomandazioni, il GEPD può esercitare i poteri conferitigli dall'articolo 47 del regolamento (CE) n. 45/2001.*

Le istituzioni e gli organismi si sono attenuti spontaneamente alle raccomandazioni del GEPD e finora non si è reso necessario prendere decisioni esecutive. Nella lettera formale che accompagna il proprio parere, il GEPD chiede che l'istituzione o l'organismo interessato lo informi delle misure adottate per mettere in pratica le raccomandazioni entro un periodo di tre mesi.

Il GEPD considera questo follow-up un **elemento decisivo ai fini della piena conformità** al regolamento. In linea con il proprio documento politico pubblicato di recente, dal titolo "Controllo e garanzia di conformità al regolamento (CE) n. 45/2001", il GEPD si attende che le istituzioni e gli organismi siano **chiamati a rispondere del seguito dato** a tutte le raccomandazioni. Ciò significa che devono essere considerati responsabili della loro attuazione e devono

Situazione comparativa



dimostrarlo al GEPD. Se un'istituzione o un organismo non si conforma alle raccomandazioni, può essere sottoposto a un'azione formale di esecuzione.

2.3.7. Conclusioni

I 55 pareri adottati dal GEPD hanno fornito preziose informazioni sulle operazioni di trattamento all'interno delle amministrazioni europee e hanno permesso al GEPD di avvalersi delle proprie competenze per fornire orientamenti di carattere generale in determinate aree, ad esempio riguardo alle procedure amministrative comuni, come risulta evidente nei trattamenti relativi a indagini amministrative e procedimenti disciplinari (cfr. sezione 2.7. Orientamenti tematici). Il GEPD continuerà a fornire tali orientamenti alle istituzioni e alle agenzie e a facilitare il processo di notifica dalle agenzie.

Poiché la maggior parte delle istituzioni sono arrivate al termine del processo di notifica delle operazioni di trattamento in corso nell'ambito di procedure amministrative standard, nel 2010 il GEPD ha ricevuto molte notifiche concernenti processi operativi fondamentali specifici di determinate istituzioni o agenzie.

Nel 2010 il GEPD ha conseguito un risultato eccellente per quanto riguarda il seguito dato ai pareri di controllo preventivo, chiudendo 137 fascicoli. Sarà sua cura continuare a vigilare da vicino sull'attività di follow-up, al fine di garantire che le istituzioni e le agenzie ottemperino tempestivamente e in modo soddisfacente alle sue raccomandazioni.

2.4. Reclami

2.4.1. Il mandato del GEPD

Nello svolgimento di una delle sue funzioni principali, così come previsto dal regolamento (CE) n. 45/2001, il GEPD "tratta i reclami e compie i relativi accertamenti" e "svolge indagini di propria iniziativa o in seguito a un reclamo" (articolo 46).

In linea di principio, una persona può presentare un reclamo soltanto in caso di presunta violazione dei suoi diritti in relazione alla protezione dei dati personali. Solo il personale dell'UE può presentare un reclamo concernente una presunta violazione delle norme in materia di protezione dei dati, indipendentemente dal fatto che il trattamento riguardi direttamente l'autore del reclamo oppure no. Lo statuto dei funzionari dell'Unione europea consente anche la presentazione di reclami al GEPD (articolo 90, lettera b).

Ai sensi del regolamento, il GEPD può compiere accertamenti soltanto sui reclami presentati da **persone fisiche**, mentre non può farlo sui reclami presentati da società commerciali o altre persone giuridiche.



Chiunque può sottoporre al GEPD reclami contro il trattamento di dati personali da parte dell'amministrazione dell'Unione europea.

Gli autori dei reclami devono fornire le proprie generalità, e pertanto le richieste anonime non sono considerate reclami. Tuttavia, le informazioni trasmesse in via anonima possono essere prese in considerazione nel quadro di un'altra procedura (come un'indagine avviata autonomamente, una richiesta di notifica di un'operazione di trattamento dati, eccetera).

Un reclamo inviato al GEPD può riguardare soltanto il trattamento di dati personali.

Il GEPD non è competente a trattare casi di cattiva amministrazione generale, modificare il contenuto dei documenti che l'autore del reclamo vuole contestare né concedere risarcimenti finanziari di danni.

*Il trattamento di dati personali oggetto di reclamo deve essere eseguito da **una delle istituzioni o uno degli organismi comunitari**. Inoltre, il GEPD non è un'istanza di appello rispetto alle decisioni delle autorità nazionali di protezione dei dati.*

2.4.2. Procedura per la gestione dei reclami

Il GEPD gestisce i reclami in conformità del quadro giuridico vigente, dei principi generali della legislazione comunitaria nonché delle buone pratiche amministrative comuni alle istituzioni e agli organismi comunitari. Nel dicembre 2009 il GEPD ha adottato un **manuale interno** per fornire al personale orientamenti sulla gestione dei reclami.

Un funzionario della Commissione europea aveva presentato reclamo contro il contenuto della relazione di valutazione stilata su di lui dal suo superiore gerarchico e chiesto al GEPD di ordinare alla Commissione di modificarla perché conteneva i suoi dati personali. Il GEPD non ha accolto le argomentazioni del reclamante. Infatti, sebbene i dati relativi alla valutazione siano dati personali, essi riguardano, per definizione, valutazioni soggettive che non possono essere modificate automaticamente sulla base delle norme sulla protezione dei dati. Per ricorrere contro l'inserimento di dati personali è necessario seguire un'apposita procedura, specificamente prevista per contestare il contenuto di relazioni di valutazione.

Inoltre, il GEPD ha applicato uno **strumento statistico** destinato al controllo delle attività collegate ai reclami, in particolare dei progressi compiuti in casi specifici.

In tutte le fasi di gestione di un reclamo, il GEPD si attiene ai principi di proporzionalità e ragionevolezza. Guidato dai principi di trasparenza e non discriminazione, egli compie le azioni opportune tenendo conto:

- della natura e gravità della presunta violazione delle norme sulla protezione dei dati;
- della rilevanza del pregiudizio che uno o più interessati possono aver subito a causa della violazione;
- della potenziale importanza generale del caso in relazione agli altri interessi pubblici e/o privati coinvolti;
- della probabilità di accertare che la violazione denunciata sia stata realmente commessa;
- della data esatta dei fatti, di qualsiasi comportamento che non produca più effetti, dell'eliminazione di questi effetti o di una garanzia adeguata della loro eliminazione.

Una persona aveva chiesto al GEPD se poteva avere accesso ai dati personali di altri partecipanti a una procedura di selezione del personale, o se tale accesso le poteva essere negato per motivi di protezione dei dati. Il GEPD non ha preso posizione perché la domanda era puramente ipotetica, considerato che l'organismo comunitario in questione non aveva ancora negato l'accesso alle informazioni richieste e pertanto non aveva ancora addotto la protezione dei dati come motivo per giustificare un rifiuto.

In linea di principio, un reclamo è **inammissibile** se il suo autore **non ha prima contattato l'istituzione interessata** per correggere la situazione. Se l'istituzione non è stata contattata, l'autore del reclamo deve fornire al GEPD motivi sufficienti a giustificare tale omissione.

Se la questione è già al vaglio di organi amministrativi – ad esempio, se è in corso un'inchiesta interna da parte dell'istituzione interessata – il reclamo è in linea di principio ammissibile. Tuttavia, il GEPD può decidere, sulla base delle particolari circostanze del caso, di attendere l'esito delle procedure amministrative in atto, prima di avviare proprie indagini. Se, invece, la stessa questione (stesse circostanze di fatto) è già stata esaminata da un tribunale, il reclamo è considerato inammissibile.

Ogni reclamo ricevuto dal GEPD viene esaminato con attenzione. L'esame preliminare del reclamo mira specificamente a verificare se esso soddisfa le condizioni per un'indagine più approfondita e se sussistono motivi sufficienti per giustificare un'indagine.

Un reclamo **che non rientra nella competenza giuridica** del GEPD è giudicato inammissibile e il suo autore viene conseguentemente informato. In casi del genere, ove pertinente, il GEPD può consigliare all'autore del reclamo di sottoporre la questione a un'altra autorità, che sia competente in materia (ad esempio, la Corte di giustizia, il Mediatore, le autorità nazionali di protezione dei dati, eccetera).

Non viene dato seguito a reclami riguardanti fatti **manifestamente irrilevanti** o che richiederebbero **sforzi d'indagine sproporzionati**. Il GEPD può compiere indagini solo su reclami concernenti violazioni **reali o potenziali**, non puramente ipotetiche, delle pertinenti norme sul trattamento dei dati personali. In tale contesto, il GEPD può valutare opzioni alternative per affrontare la questione in esame, o da parte dell'autore del reclamo o da parte del GEPD stesso. Per esempio, il GEPD può avviare di propria iniziativa un'indagine su un problema di carattere generale, oppure su un caso specifico sottoposto dall'autore di un reclamo. In queste circostanze, l'autore del reclamo viene informato di tutti gli strumenti di azione disponibili.

Al fine di assicurare un trattamento uniforme dei reclami riguardanti la protezione dei dati, nonché di evitare inutili doppioni, il **Mediatore europeo** e il GEPD hanno firmato nel novembre 2006 un protocollo d'intesa il quale prevede, tra l'altro, che un reclamo già esaminato non possa essere riaperto da un'altra istituzione, a meno che non vengano prodotte nuove prove significative.

Per quanto attiene ai **limiti di tempo**, un reclamo è in linea di principio inammissibile se viene sottoposto al GEPD oltre due anni dopo la data nella quale l'autore del reclamo è venuto a conoscenza dei fatti.

Qualora il reclamo sia ammissibile, il GEPD avvia **un'indagine** che comprende l'invio di una richiesta d'informazioni all'istituzione interessata, un riesame

dei documenti pertinenti, un incontro con il responsabile del trattamento, un'ispezione in loco, eccetera. Il GEPD ha il potere di ottenere dall'autorità o dall'organismo interessati l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'indagine. Può altresì avere accesso a qualsiasi sede in cui un responsabile del trattamento o un'istituzione/un organismo svolgano le proprie attività.

Al termine dell'indagine, all'autore del reclamo e al responsabile del trattamento dei dati sarà inviata una **decisione** nella quale il GEPD esprime il proprio parere riguardo a eventuali violazioni delle

norme sulla protezione dei dati da parte dell'istituzione in questione. I **poteri del GEPD** sono ampi e vanno dalla semplice formulazione di consigli agli interessati ad avvertenze o ammonimenti al responsabile, fino all'imposizione di un divieto di trattamento o al deferimento della questione alla Corte di giustizia.

Qualsiasi parte interessata può chiedere al GEPD di **rivedere** una sua decisione entro un mese dall'adozione della stessa. Le parti interessate possono anche presentare appello direttamente alla Corte di giustizia.

Nel 2009, in due occasioni sono state impugnate di fronte alla Corte di giustizia due decisioni del GEPD (cause T-164/09 e T-193/09). Nella prima causa, la Corte ha deciso per il non luogo a procedere nei confronti della decisione del GEPD perché era venuta meno la finalità dell'azione. Nella seconda causa, la Corte ha respinto la domanda dell'appellante senza discuterne nel merito.

2.4.3. Garanzia di riservatezza agli autori dei reclami

*Il GEPD riconosce che taluni autori di reclami mettono a repentaglio la loro carriera quando denunciano violazioni delle norme sulla protezione dei dati. Pertanto, è doveroso garantire la **riservatezza** degli autori dei reclami e degli informatori che la richiedano. Dall'altro canto, però, il GEPD è tenuto a operare in **maniera trasparente** e a rendere pubblica quanto meno la sostanza delle proprie decisioni. Le procedure interne del GEPD riflettono l'esigenza di assicurare questo difficile equilibrio.*

È politica abituale del GEPD trattare i reclami in regime di riservatezza. Tale **trattamento riservato** significa che le informazioni personali non sono rivelate a persone esterne al GEPD. Tuttavia, ai fini di un'adeguata esecuzione dell'indagine può essere necessario informare i servizi competenti dell'istituzione interessata e i terzi coinvolti del contenuto del reclamo e dell'identità del suo autore. Inoltre, il GEPD mette in copia il responsabile della protezione dei dati (RPD) dell'istituzione interessata in tutta la propria corrispondenza con l'istituzione.

Se l'autore del reclamo chiede che sia garantito il proprio **anonimato** nei confronti dell'istituzione, dell'RPD o dei terzi coinvolti, viene invitato a motivare tale richiesta. Il GEPD valuta le argomentazioni dell'autore del reclamo e le conseguenze della richiesta per la fattibilità della propria indagine.

Se decide di non concedere l'anonimato, spiega i motivi di tale decisione e chiede all'autore del reclamo se accetta che il GEPD esamini il reclamo senza garantire l'anonimità, o se preferisce ritirare il reclamo. In questo secondo caso, l'istituzione interessata non viene informata della presentazione del reclamo e il GEPD può adottare altre azioni senza rivelarla all'istituzione interessata (ad esempio, può avviare un'indagine di propria iniziativa o chiedere una notifica riguardo a un'operazione di trattamento di dati).

Al termine dell'indagine, **tutti i documenti concernenti il reclamo**, compresa la decisione finale, sono trattati in linea di principio in modo riservato: non vengono pubblicati integralmente né trasferiti a terzi. Una sintesi anonima del reclamo può, però, essere pubblicata dal GEPD sul proprio sito e nella relazione annuale, in forma tale da non consentire l'identificazione dell'autore del reclamo né dei terzi coinvolti. In casi importanti, il GEPD può anche decidere di rendere pubblica per esteso la propria decisione finale, ma dovrà comunque tenere in considerazione la richiesta di riservatezza dell'autore del reclamo e, quindi, dovrà agire in modo tale da non consentire l'identificazione dell'autore del reclamo né di altre persone interessate.

2.4.4. Reclami esaminati nel corso del 2010

2.4.4.1. Numero dei reclami

La complessità dei reclami ricevuti dal GEPD è aumentata nel 2010, mentre il loro numero è diminuito. **Nel 2010 il GEPD ha ricevuto 94 reclami** (con un calo del 15% rispetto al 2009). Di essi, **69 erano inammissibili** e la maggioranza di essi riguardava il trattamento di dati a livello nazionale in contrapposizione al trattamento da parte di un'istituzione o un organismo comunitario.

I restanti 25 reclami hanno richiesto indagini più approfondite (con un calo del 41% rispetto al 2009). Inoltre, 18 reclami ammissibili presentati in anni precedenti (16 nel 2009 e due nel 2008) nel 2010 erano ancora in fase di indagine o revisione.

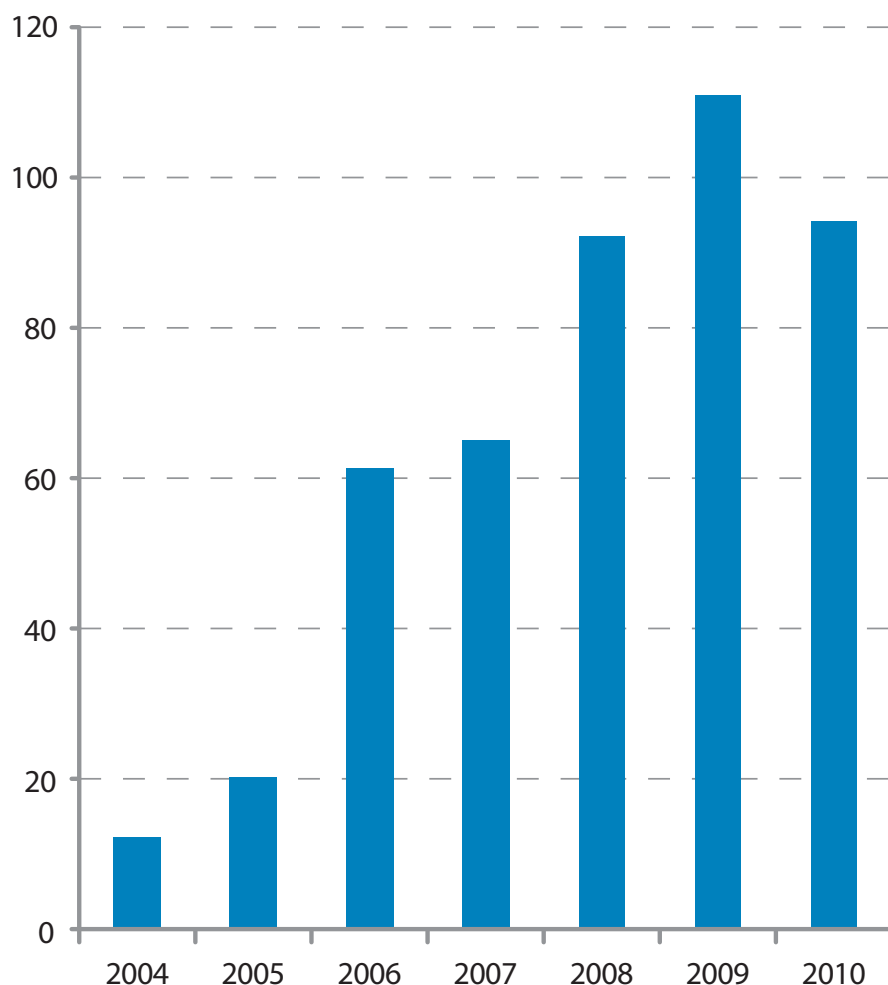
2.4.4.2. Tipologia degli autori dei reclami

Dei 94 reclami ricevuti, 17 (18%) erano stati presentati da dipendenti di istituzioni o organismi comunitari, compresi ex dipendenti e candidati all'assunzione, mentre gli autori dei restanti 77 reclami non risultavano avere un rapporto di lavoro con l'amministrazione dell'Unione europea.

2.4.4.3. Istituzioni interessate dai reclami

Dei reclami ammissibili presentati nel 2010, la maggioranza (80%) erano contro la **Commissione europea, compresi l'OLAF e l'EPSO**, il che non sorprende, ove si consideri che la Commissione compie un maggior numero di operazioni di trattamento dati rispetto alle altre istituzioni e organismi comunitari. Il numero relativamente elevato dei reclami riguardanti l'OLAF e l'EPSO si può spiegare con la natura delle loro attività.

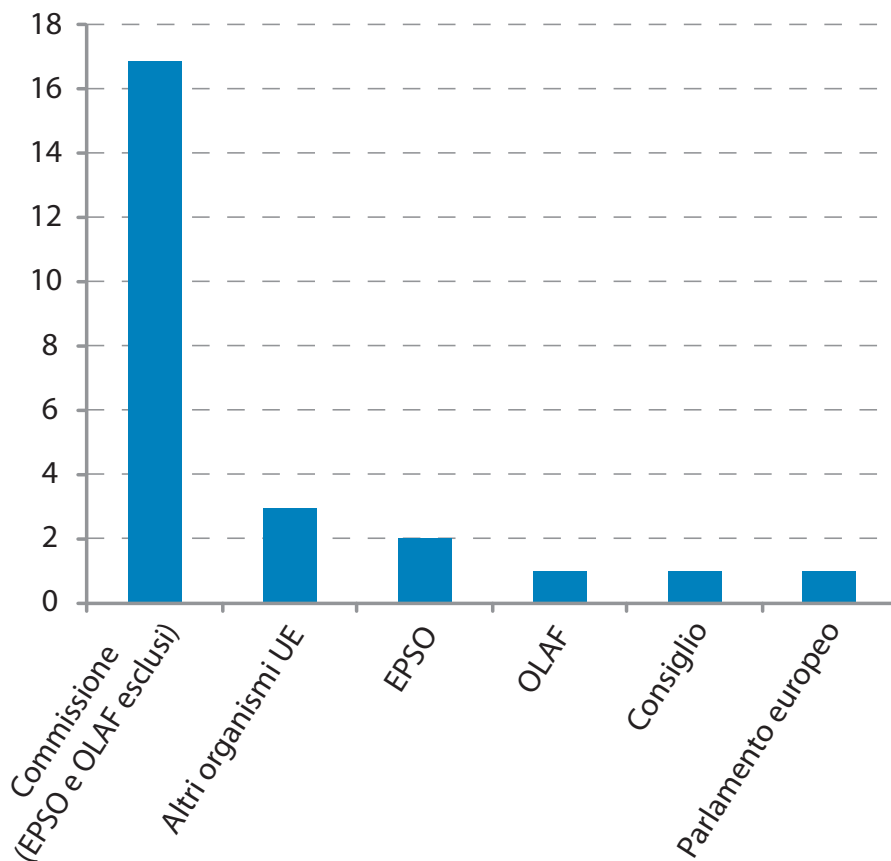
Numero di reclami ricevuto (andamento 2004-2010)



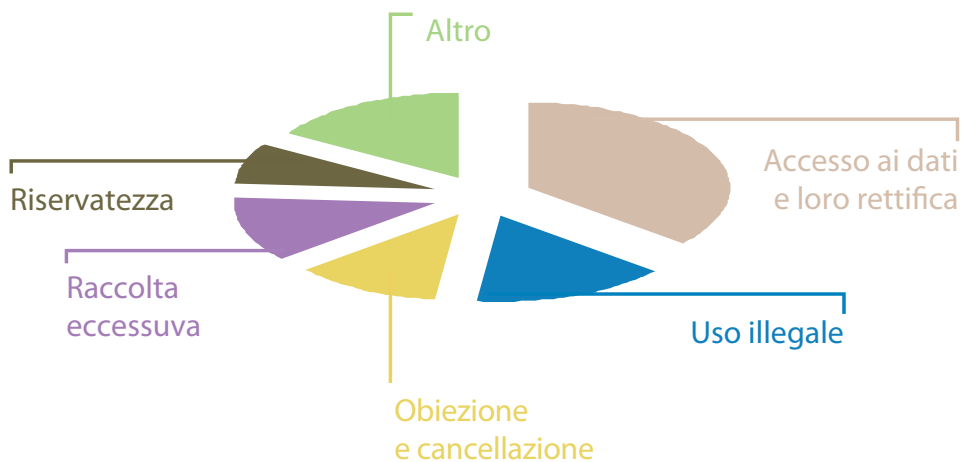
2.4.4.4. Lingua dei reclami

La maggior parte dei reclami sottoposti erano redatti in inglese (44%) o tedesco (33%), mentre il francese (15%) è meno usato. I reclami in altre lingue sono relativamente infrequenti (8%).

Istituzioni e organismi comunitari interessati



Tipi di violazioni denunciate



2.4.4.5. Tipi di violazioni denunciate

Le violazioni delle norme di protezione dei dati denunciate dagli autori di reclami nel 2010 riguardavano principalmente:

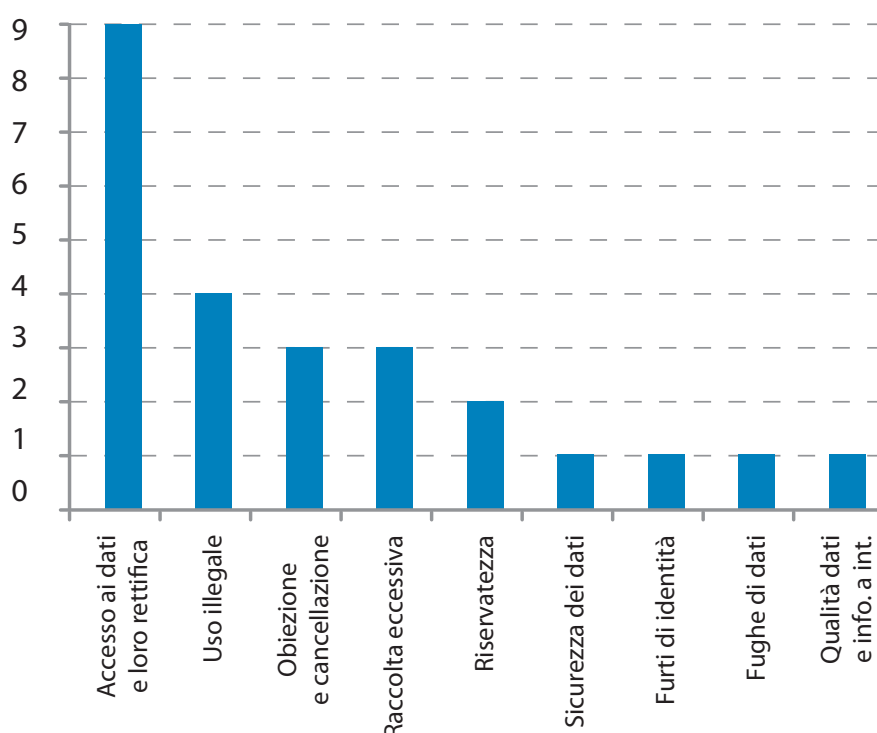
- violazioni dei diritti degli interessati, come l'accesso ai dati e la loro rettifica (36%) o l'obiezione e la cancellazione (12%);
- l'uso illegale (16%), la raccolta eccessiva di dati personali (12%), violazioni della riservatezza (8%).

Altre presunte violazioni meno frequenti riguardano la sicurezza dei dati (4%), furti di identità (4%), fughe di dati (4%), qualità dei dati e informazioni fornite agli interessati (4%).

2.4.4.6. Risultati delle indagini del GEPD

In 10 casi risolti nel corso del 2010, il GEPD ha riscontrato che non c'era stata violazione delle norme sulla protezione dei dati.

Risultati delle indagini del GEPD



Il GEPD ha ricevuto un reclamo riguardante l'accesso al fascicolo sanitario tenuto dal servizio medico di un'istituzione. Il GEPD ha confermato che, ai sensi delle norme sulla protezione dei dati, il diritto di accedere ai dati personali non significa che il responsabile del trattamento sia obbligato a inviare il documento medico originale, bensì che l'interessato può, in pratica, prenderne visione (di persona o, in certi casi, indirettamente tramite un medico) e/o farne copie. In merito al diritto di rettificare dati inesatti o incompleti, il GEPD ha precisato che l'obbligo di rettificare dati sanitari vale solo per i dati di fatto, non per le valutazioni riguardanti lo stato di salute. Pertanto, in conformità delle norme sulla protezione dei dati, il responsabile non è tenuto a modificare le conclusioni di un rapporto medico. Stando così le cose, il diritto di rettificare i dati potrebbe risultare nell'impossibilità di aggiungere altri rapporti stilati da altri medici e contenenti valutazioni differenti. Il GEPD ha quindi concluso che in quel caso non c'era stata alcuna violazione delle norme sulla protezione dei dati.

Per contro, in 11 casi è stato accertato il mancato adempimento delle norme sulla protezione dei dati e sono state formulate raccomandazioni al responsabile del trattamento.

Il GEPD ha ricevuto un reclamo concernente la pubblicazione nella Gazzetta ufficiale dell'Unione europea e nei verbali di una sessione del Parlamento europeo di dati personali estremamente sensibili. Dopo aver condotto un'indagine, il GEPD ha concluso che il parere del parlamentare e il messaggio della dichiarazione scritta avrebbero potuto essere espressi in maniera efficace senza che fosse rivelata l'identità delle persone interessate. Il GEPD ha chiesto la cancellazione, dalla dichiarazione scritta e da ogni altro mezzo di comunicazione, dei nomi delle persone citate dal parlamentare; ha chiesto altresì che fosse stabilita una procedura formale ed efficace per garantire che le versioni definitive dei documenti pubblicati nella Gazzetta ufficiale e sul sito del Parlamento europeo tenessero conto delle rettifiche apportate dai servizi preposti alla redazione di documenti.

Il GEPD ha ricevuto un reclamo concernente la comunicazione dei numeri personali dei dipendenti di un'agenzia a tutti gli utenti, attraverso gli indirizzi di posta elettronica interni dell'agenzia stessa. Questa operazione, che ha comportato il trattamento di dati personali, aveva lo scopo di invitare tutti i dipendenti a un appuntamento con la sezione responsabile della sicurezza dell'agenzia per sottoporsi a una seduta fotografica. Il GEPD ha ritenuto che, considerata tale finalità, sarebbe stato del tutto sufficiente inviare un elenco contenente solo il nome e il cognome delle persone interessate. L'indicazione del numero personale era irrilevante ed eccessiva rispetto alle finalità del trattamento e costituiva pertanto una violazione dell'articolo 4 del regolamento. Il GEPD ha invitato l'agenzia a ordinare formalmente al personale che gestisce i dati personali di operare con maggiore selettività e di prestare particolare attenzione nel caso di invii massicci di corrispondenza interna o esterna contenente dati personali, al fine di garantire che nei messaggi compaiano solamente i dati necessari per le finalità dei messaggi stessi.

Un dipendente ha presentato un reclamo in cui denunciava il ricorso a videosorveglianza occulta nell'istituzione per cui lavorava. In particolare, contestava la liceità dell'utilizzo di una videocamera che lo riprendeva, a sua insaputa, quando entrava nell'ufficio del proprio supervisore in sua assenza. Il GEPD ha concluso che l'istituzione non aveva dimostrato l'esistenza di una base giuridica che autorizzasse esplicitamente operazioni altamente invasive come quella denunciata e stabilisse condizioni e tutele specifiche. Senza una base giuridica trasparente e senza un approccio strutturato, la proporzionalità della videosorveglianza occulta era dubbia. Pertanto, il GEPD ha invitato l'istituzione interessata a valutare se intendeva servirsi della videosorveglianza occulta anche in futuro e, in caso positivo, a presentare al GEPD i suoi progetti in tal senso per un controllo preventivo.

2.4.5. Altre attività nel campo dei reclami

Il GEPD vuole facilitare la procedura di presentazione dei reclami e accelerare la loro gestione da parte dei propri servizi mettendo a disposizione sul sito un **modulo di presentazione dei reclami online** (cfr. sezione 5.6.1). Una versione provvisoria del modulo è disponibile sul sito del GEPD dall'inizio del 2010. La versione finale sarà più interattiva. Il GEPD si aspetta che un utilizzo generalizzato di questa applicazione aiuti coloro che intendono presentare reclami a valutare l'ammissibilità della loro richiesta e quindi a sottoporre all'attenzione del GEPD solo questioni pertinenti. Inoltre, il GEPD si augura di ottenere informazioni più ampie e rilevanti per gestire i reclami con maggiore efficienza e ridurre il numero dei reclami manifestamente inammissibili.

Il GEPD intende altresì procedere a una revisione del manuale interno per la gestione dei reclami adottato nel 2009. Le procedure modificate andranno a integrare la nuova struttura organizzativa del GEPD e renderanno più chiaro il flusso di lavoro interno dei reclami.

2.5. Controllo di conformità

*Il GEPD ha la responsabilità di controllare e **garantire l'applicazione del regolamento (CE) n. 45/2001**. Il controllo è stato effettuato perlopiù attraverso un **esercizio di rendicontazione** denominato "Primavera 2009". Accanto a questo esercizio di rendicontazione generale, sono stati eseguiti esercizi di controllo mirati nei casi in cui il GEPD, a seguito delle proprie attività di vigilanza, nutiva dubbi quanto al grado di conformità di istituzioni o organismi specifici. Alcuni di questi controlli sono avvenuti in via epistolare, altri in forma di **visite** di un giorno all'organismo interessato, allo scopo di affrontare le situazioni di non conformità; infine, in alcune istituzioni e organismi sono state compiute **ispezioni** per accertare la conformità in merito a questioni specifiche.*

2.5.1. Controllo mirato ed esercizi di rendicontazione

Il GEPD ha avviato esercizi di controllo mirati, in via epistolare, nei casi in cui nutriva dubbi sulla conformità al regolamento da parte di un'istituzione o un organismo riguardo a determinate questioni. A titolo d'esempio si possono citare il controllo sulle indagini amministrative interne della Banca centrale europea e quello sulle operazioni di trattamento presso la DG Relazioni esterne.

Indagini amministrative interne – Banca centrale europea

Nel gennaio 2010 il GEPD ha aperto un'indagine sulla protezione dei dati personali durante le indagini amministrative interne presso la Banca centrale europea (BCE). La relativa decisione è stata adottata in virtù dell'articolo 46, lettera b), del regolamento, a titolo di follow-up del parere del GEPD del 22 dicembre 2005 riguardante tali indagini all'interno della BCE. L'indagine del GEPD si è concentrata sul possibile accesso a file elettronici e sull'intercettazione di conversazioni telefoniche. Alla BCE sono state inviate varie domande sull'applicazione della sua circolare amministrativa 01/2006 concernente le indagini amministrative interne e i relativi principi. Tali domande riguardavano, tra l'altro, le modalità di documentazione della procedura, l'esistenza o meno di un protocollo informatico forense e di statistiche annuali per l'intercettazione di conversazioni telefoniche, nonché l'accesso a file elettronici e dati sul traffico. L'inchiesta non si è ancora conclusa.

L'inventario della DG Relazioni esterne

Sollecitato da un certo numero di reclami, il GEPD ha cominciato a dubitare che l'inventario delle operazioni di trattamento eseguite sotto il controllo della DG Relazioni esterne riportasse accuratamente le operazioni di trattamento riguardanti dati personali all'interno delle delegazioni dell'UE. Il GEPD voleva inoltre avere conferma del fatto che la DG Relazioni esterne avesse notificato all'RPD della Commissione tutte le operazioni di trattamento delle delegazioni dell'UE, conformemente all'articolo 25. La DG Relazioni esterne ha successivamente fornito aggiornamenti e garanzie appropriate su entrambe le questioni sollevate e il caso è stato chiuso.

Visita all'Agenzia europea per la sicurezza delle reti e dell'informazione

Il 17 settembre 2010 il GEPD ha compiuto una visita presso l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) per verificare e discutere il basso livello di conformità al regolamento (CE) n. 45/2001. La visita è stata decisa alla luce delle prove raccolte durante le attività di vigilanza del GEPD, consistenti in un reclamo, una richiesta di consulenza e nella mancanza di seguito a un parere di controllo preventivo.

La visita ha inoltre permesso al responsabile della protezione dei dati di aggiornare il GEPD sui progressi compiuti dall'ENISA, compresa l'istituzione di un registro elettronico, un meccanismo di follow-up e un nuovo inventario. L'RPD ha sottolineato come, nello svolgimento delle proprie funzioni, incontri difficoltà a tutelare la propria indipendenza, mentre il Garante aggiunto ha citato il documento sugli standard professionali per gli RPD (adottato nel frattempo – ottobre 2010), che dovrebbe aiutare gli RPD a potenziare e chiarire il loro ruolo all'interno dei rispettivi organismi.

Nella riunione conclusiva le due parti hanno concordato, sulla base dei requisiti del GEPD, un programma di vigilanza (con scadenze specifiche) che sottolinea l'importanza dei tre principali strumenti di conformità al regolamento: l'inventario, il registro e le notifiche al GEPD previste dall'articolo 27. Il Garante seguirà da vicino i progressi che l'ENISA compirà rispetto a questo programma, al fine di garantire la conformità al regolamento.

Visita all'Agenzia europea dell'ambiente

Il 10 dicembre 2010 il GEPD ha compiuto una visita presso l'Agenzia europea dell'ambiente (EEA) per verificare e discutere il livello di conformità al regolamento da parte dell'Agenzia.

Durante la visita ci sono stati un incontro tra il GEPD e il direttore dell'EEA nonché altri incontri ai quali hanno partecipato il responsabile della protezione dei dati e i controllori delle operazioni di trattamento. Tali incontri hanno offerto al GEPD l'opportunità di manifestare le proprie preoccupazioni per l'attuale livello di conformità dell'EEA e ha permesso a quest'ultima di aggiornarlo sui progressi compiuti verso il conseguimento della piena conformità. In tale contesto, il GEPD ha preso atto con piacere dei notevoli sforzi fatti di recente dall'Agenzia e del suo impegno ad ovviare alle proprie carenze.

Le parti hanno concordato un programma di conformità (con scadenze specifiche) la cui attuazione sarà controllata da vicino dal GEPD.

2.5.2. Controllo e rendicontazione generale: esercizio "Primavera 2009"

Sulla scia dell'esercizio di controllo generale lanciato nella primavera del 2009, il GEPD ha continuato a monitorare l'applicazione delle norme e dei principi della protezione dei dati da parte delle istituzioni e degli organismi interessati.

Le **istituzioni comunitarie** hanno continuato a compiere **significativi progressi** per quanto attiene al soddisfacimento dei requisiti di protezione dei dati e, sebbene anche altri organismi abbiano ottenuto miglioramenti, in linea generale è stato riscontrato un **più basso livello di conformità** all'interno delle **agenzie**.

Nei casi in cui il GEPD ha ritenuto che i progressi in termini di conformità fossero insufficienti, sono stati fissati obiettivi adeguati. Purtroppo, in alcuni casi questi obiettivi non sono stati conseguiti e, di conseguenza, il GEPD ha chiesto ulteriori aggiornamenti. Laddove gli aggiornamenti non sono stati forniti o i progressi erano troppo lenti, il GEPD ha avviato esercizi di controllo più mirati (cfr. sopra).

Aggiornamenti dell'esercizio Primavera 2009

- **Notifica di operazioni di trattamento dai controllori dei dati all'RPD:** complessivamente, il livello delle notifiche è cresciuto e il GEPD, pur continuando a chiedere aggiornamenti sui progressi, si occuperà anche delle istituzioni e degli organismi che hanno prestazioni insoddisfacenti, conformemente al documento politico che ha pubblicato di recente in materia di controllo e garanzia della conformità.
- **Notifica di operazioni di trattamento al GEPD per controllo preventivo:** a tale proposito, la maggior parte delle istituzioni hanno compiuto significativi progressi, sebbene anche in questo campo le agenzie registrino livelli di conformità più bassi. Pertanto, l'anno prossimo il Garante cercherà di affrontare questo problema.

2.5.3. Prossimi passi

Il GEPD incoraggerà e controllerà da vicino ulteriori progressi, specialmente nelle istituzioni e agenzie che devono migliorare la conformità per quanto attiene ai controlli preventivi del GEPD e alle notifiche al responsabile della protezione dei dati. Il Garante continuerà inoltre a sottolineare l'utilità di un **inventario** e di una **procedura interna di follow-up per le proprie raccomandazioni** ai fini della conformità al regolamento.

Il prossimo esercizio di controllo generale (**Primavera 2011**) comincerà all'inizio del 2011, ma è probabile che siano portate avanti ulteriori iniziative mirate concernenti la conformità, visti i risultati ottenuti negli esercizi precedenti.

2.5.4. Ispezioni

Le ispezioni sono uno strumento fondamentale che consente al GEPD di controllare e garantire l'applicazione del regolamento. La loro base giuridica sono gli articoli 41, paragrafo 2, 46, lettera c), e 47, paragrafo 2.

Gli ampi poteri del GEPD di accedere a qualsiasi informazione e dato personale necessari per le indagini e di avere accesso a qualsiasi sede in cui il responsabile del trattamento o l'istituzione o l'organismo svolgano la propria attività sono stati previsti al fine di assicurare che il GEPD disponga di strumenti sufficienti per svolgere i propri compiti. Le ispezioni possono essere avviate a seguito di un reclamo o su iniziativa propria del GEPD.

L'articolo 30 del regolamento richiede alle istituzioni e agli organismi dell'UE di collaborare con il GEPD nell'esercizio delle sue funzioni e di fornire le informazioni e gli accessi richiesti.

Durante le ispezioni, il GEPD **verifica i fatti in loco** con l'ulteriore fine di assicurare la conformità. Le

ispezioni sono seguite da un adeguato riscontro nei confronti dell'istituzione o dell'organismo sottoposto a ispezione.

Nel 2010 il GEPD ha proseguito il follow-up di ispezioni precedenti e, nel dicembre 2010, ha eseguito un'ispezione presso il Centro comune di ricerca della Commissione a Ispra.

Seguito dato all'ispezione presso l'Ufficio europeo di selezione del personale

Nel marzo 2009 il GEPD ha compiuto un'ispezione presso l'Ufficio europeo di selezione del personale (EPSO), allo scopo di trovare riscontri fattuali di numerose operazioni di trattamento che erano state oggetto di controlli preventivi e riguardavano la selezione di funzionari, dipendenti temporanei e agenti a contratto, nonché tutte le relative operazioni di trattamento dei dati personali. Il GEPD ha tratto una serie di conclusioni, con particolare riguardo alla trasparenza delle procedure dell'EPSO e alla conservazione dei dati. Successivamente l'EPSO ha tenuto conto di tali conclusioni.



Le ispezioni sono uno strumento essenziale per controllare e assicurare l'applicazione del regolamento sulla protezione dei dati.

L'ispezione aveva anche lo scopo di garantire la conformità delle **banche dati dell'EPSO e degli strumenti informatici selezionati** che erano stati utilizzati nelle procedure di selezione. Il GEPD è tuttora in attesa di ulteriori riscontri sui progressi compiuti nell'ambito del piano di implementazione delle proprie raccomandazioni e ha pertanto rinviato la formulazione delle conclusioni finali sull'ispezione, in attesa di queste informazioni.

Seguito dato all'ispezione presso la Corte dei conti europea

Dopo l'ispezione del GEPD presso la Corte dei conti europea nel marzo 2009 in relazione al **controllo del personale** (monitoraggio Internet e relazione sullo strumento di audit), la collaborazione avviata con la Corte è stata proficua e il Garante ha potuto registrare progressi riguardo alla conformità sui temi esaminati.

In merito al **monitoraggio dell'utilizzo di Internet** (fascicolo 2008-0284), il GEPD ha formulato raccomandazioni specifiche nella relazione concernente il seguito dato al proprio parere. Sono ancora in corso ulteriori discussioni al fine di garantire la piena conformità nel quadro generale dell'analisi di tale questione all'interno del contesto istituzionale.

Per quanto attiene alla consultazione su una procedura per accedere all'unità/posta elettronica privata dei dipendenti, il GEPD ha stabilito che gli doveva essere inviata una notifica formale di controllo preventivo di questa operazione di trattamento, perché essa comportava un rischio specifico ai sensi dell'articolo 27, paragrafo 1, del regolamento. Nel gennaio 2010 il GEPD ha adottato un parere in proposito (fascicolo 2009-0620) con il quale autorizzava le operazioni di trattamento a condizione che fossero rispettate alcune raccomandazioni specifiche, che la Corte dei conti ha successivamente attuato. Pertanto, il GEPD ha chiuso il caso.

Seguito dato all'ispezione della s-TESTA

La rete s-TESTA (Rete di servizi transeuropei per la comunicazione telematica tra amministrazioni) fornisce un'infrastruttura generica che risponde alle esigenze commerciali e ai requisiti dello scambio di informazioni delle amministrazioni europee e nazionali. Attualmente, oltre trenta applicazioni fanno affidamento su questa rete sicura messa a disposizione dalla Commissione europea.

Nel gennaio 2010 il GEPD ha adottato un parere contenente 22 raccomandazioni relative all'ispezione condotta presso il Centro operativo e di servizi della s-TESTA. Nel dicembre 2010 la Commissione ha inviato al GEPD una relazione di attuazione riguardante tali raccomandazioni nella quale comunicava che dodici di esse erano già state messe in atto, mentre le altre dieci, che necessitavano di ulteriori e significativi investimenti, erano state inserite nel piano di miglioramento continuo del sistema e sarebbero state attuate nel 2011. Il GEPD verificherà questi aspetti ancora in sospeso nel corso di un'azione di follow-up programmata per la metà del 2011.

Ispezione presso il Centro comune di ricerca

Nel dicembre 2010 il GEPD ha compiuto un'ispezione in loco presso il Centro comune di ricerca di Ispra. Una generalizzata mancanza di collaborazione da parte del Centro, unita alla necessità di verificare lo stato reale e controllare in loco l'attuazione delle proprie raccomandazioni, hanno indotto il GEPD a svolgere questa ispezione.

Essa ha riguardato due aree principali: la selezione e assunzione del personale del Centro e le procedure messe in atto dal servizio di sicurezza (controlli di sicurezza pre-assunzione, indagini di sicurezza, controllo dell'accesso e registrazione di chiamate di emergenza). In tutti questi casi le informazioni generali erano state ricavate da analisi di controllo preventivo.

Durante l'ispezione, la collaborazione tra il GEPD e le unità interessate del Centro è stata proficua e ha permesso agli ispettori di giungere alla conclusione, tra l'altro, che la causa principale della mancanza di collaborazione registrata in passato risiedeva in problemi di comunicazione. Alla luce dei risultati, il GEPD stilerà una relazione di ispezione con nuove raccomandazioni, per assicurare una migliore conformità al regolamento.

2.6. Consultazioni su misure amministrative

2.6.1. Consultazioni ai sensi degli articoli 28, paragrafo 1, e 46, lettera d)

Il regolamento (CE) n. 45/2001 sancisce il diritto del GEPD di essere informato sulle misure amministrative riguardanti il trattamento di dati personali (articolo 28, paragrafo 1). Il GEPD può emettere un parere su richiesta dell'istituzione o dell'organismo interessato oppure di propria iniziativa.

Il termine “misura amministrativa” significa una decisione adottata dall'amministrazione che si applica, con validità generale, al trattamento dei dati personali effettuato dall'istituzione o dall'organismo interessato (ad esempio, le misure di applicazione del regolamento, disposizioni e politiche interne generali o le decisioni adottate dall'amministrazione in materia di trattamento dei dati personali).

Inoltre, l'articolo 46, lettera d), del regolamento prevede un ambito di applicazione molto vasto delle consultazioni, tale da includere “qualsiasi argomento relativo al trattamento di dati personali”. Questa è la base giuridica del potere consultivo del GEPD nei confronti di istituzioni e organismi su casi specifici concernenti attività di trattamento dei dati o su questioni generali di interpretazione del regolamento.

Nel contesto delle consultazioni sulle misure amministrative previste da un'istituzione o un organismo sono stati esaminati vari argomenti, alcuni dei quali sono illustrati in prosieguo.

2.6.2. Richiesta di accesso all'identità di un informatore – Mediatore europeo

Il Mediatore europeo ha consultato il GEPD su una questione sollevata in un reclamo presentato contro l'OLAF. La consultazione comprendeva una serie di interrogativi, quali:

- se l'identità delle persone che forniscono informazioni all'OLAF, come informatori o informatori interni, non debba essere rivelata a nessuno tranne che all'autorità giudiziaria;

- se la protezione di informatori e informatori interni debba essere garantita anche dopo la chiusura di un'indagine senza follow-up e, se sì, come e in quale misura.

Il GEPD ha espresso commenti sulle norme o sulla politica, non sullo specifico reclamo presentato contro l'OLAF. Il GEPD ha sostenuto che, in linea generale, l'identità di un informatore o informatore interno non deve essere svelata, tranne nel caso in cui ciò comporti una violazione delle norme nazionali di procedura giudiziaria e/o tali persone facciano dolosamente dichiarazioni false. In questi casi, i dati personali possono essere rivelati soltanto alle autorità giudiziarie.

In merito al secondo interrogativo, il GEPD ha concluso che sussistono validi motivi per ritenere che la protezione di informatori e informatori interni debba essere la stessa dopo la chiusura di un'indagine, indipendentemente dal fatto che ci sia un seguito oppure no. La vulnerabilità del ruolo dell'informatore o dell'informatore interno e, quindi, i rischi per la loro vita privata e la loro integrità non cambiano a seconda che l'indagine sia aperta o venga chiusa senza un seguito.

Nella pratica questo approccio non esclude, ovviamente, le situazioni nelle quali la protezione degli informatori o informatori interni debba cedere il posto alle legittime richieste di altri. Il passare del tempo può essere un fattore rilevante, ma è ovviamente difficile ragionare al riguardo in termini astratti.

2.6.3. Trasferimenti internazionali di dati personali – Agenzia europea per la sicurezza aerea

L'Agenzia europea per la sicurezza aerea (EASA) svolge alcune attività (ad esempio, servizi nel campo della certificazione) che comportano il pagamento di tasse e oneri da parte dei richiedenti. Una parte di queste attività di certificazione può essere svolta del tutto o in parte al di fuori del territorio degli Stati membri. In alcuni casi, i richiedenti hanno chiesto all'Agenzia di fornire loro i nomi e le date dei viaggi degli esperti, per poter effettuare i relativi pagamenti.

Il responsabile della protezione dei dati dell'EASA ha consultato il GEPD in merito all'applicazione dell'articolo 9 del regolamento al caso in esame.

Ai sensi dell'articolo 9, paragrafo 1, i dati personali possono essere trasferiti a destinatari diversi dalle istituzioni e dagli organismi comunitari e non soggetti alla normativa nazionale adottata in attuazione della direttiva 95/46/CE qualora nel paese del destinatario **sia assicurato un livello adeguato di protezione.**

Il GEPD ha sottolineato che, se il paese terzo in questione – non appartenente allo Spazio economico europeo – non assicura un livello adeguato di protezione, si devono prendere in considerazione le altre condizioni citate dall'articolo 9, il quale, nel paragrafo 6, stabilisce che "In deroga ai paragrafi 1 e 2, le istituzioni e gli organismi comunitari possono trasferire dati personali a condizione che: (...) d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante (...)".

Poiché in questo caso la fornitura dei servizi è una delle attività fondamentali dell'EASA, i trasferimenti eseguiti per il pagamento di tali servizi possono essere considerati, in linea di principio, **necessari per il funzionamento di questo organismo**, rientrando così nelle condizioni previste per la deroga ai sensi dell'articolo 9, paragrafo 6, lettera d).

Il GEPD ha rilevato altresì che, nel caso in esame, sembrava che i trasferimenti non sarebbero stati "ripetuti, massicci o strutturali", bensì si sarebbe trattato di un trasferimento "singolo" a destinatari diversi in paesi diversi. Quanto ai rischi per gli interessati, non sono stati citati rischi particolari, né le categorie di dati da trasferire (nomi e date dei viaggi degli esperti) sembravano tali da suscitare timori particolari.

Il GEPD ha però fatto notare che non erano previste garanzie nei casi in deroga; ha quindi raccomandato l'introduzione di una clausola per specificare che il destinatario è legittimato per legge a chiedere i dati e deve limitarne l'uso alle sole finalità del trasferimento.

2.6.4. Politica sull'uso interno della posta elettronica – Commissione europea

La Commissione europea ha consultato il GEPD in merito alla propria politica sull'uso interno della posta elettronica. Il GEPD ha analizzato i punti specifici di tale politica sotto il profilo della protezione dei dati personali e dei principi della tutela della vita privata, nonché le misure di sicurezza.

In proposito, la Commissione ha comunicato al GEPD che non compie controlli su larga scala a livello individuale. In una lettera inviata al GEPD, afferma che l'unica forma di controlli periodici eseguiti dal servizio di posta elettronica della Commissione (DG Informatica) è a livello di direzione generale/servizio, non a livello di caselle di posta personali o di dati sul traffico individuale, e che la DG Informatica controlla l'utilizzo della posta per ridurre i rischi operativi, ma non stila rapporti periodici per monitorare l'attività delle caselle di posta personali né per fornire dati sul traffico individuale da usare per l'analisi di abusi individuali.

Ciò implica che qualsiasi controllo delle caselle di posta personali può avvenire **solamente nel quadro di un'indagine in corso**. Il GEPD valuta positivamente tale approccio, che reputa essere la migliore pratica.

2.6.5. Diritti dell'amministratore informatico – Banca europea per gli investimenti

Il 26 marzo 2010 il GEPD ha risposto a una richiesta di consulenza presentata dalla Banca europea per gli investimenti (BEI) formulando raccomandazioni sulla gestione dell'accesso da parte degli amministratori informatici ai dati personali conservati nei sistemi e nelle applicazioni informatici. Il GEPD ha sottolineato l'esigenza di applicare il **principio di separazione dei compiti**. Il grado di separazione va stabilito in base al livello di rischio individuato per il processo considerato.

La gestione dei diritti di accesso dell'amministratore informatico va affrontata attraverso un approccio equilibrato fondato su misure tecniche e organizzative. Il GEPD ha altresì raccomandato che tali misure siano documentate adeguatamente in una dettagliata politica di sicurezza definita dall'istituzione.

2.6.6. Controllo delle comunicazioni telefoniche

Il GEPD è stato consultato in merito a un progetto riguardante il controllo delle comunicazioni telefoniche eccedenti una soglia prestabilita.

Il sistema previsto si fondava su una soglia prestabilita (numero tollerato di ore o costo tollerato delle comunicazioni telefoniche) che sarebbe stata offerta al personale. Alla fine di ogni mese, gli amministratori

avrebbero ricevuto un elenco degli utenti alle loro dipendenze le cui telefonate all'estero o a telefoni cellulari (privati o professionali) nel mese precedente avevano ecceduto la soglia prevista.

Il GEPD ha riconosciuto che il trattamento di questi dati è lecito in quanto è collegato all'esercizio legittimo di pubblici poteri di cui sono investiti l'istituzione o l'organismo per garantire una gestione efficiente dell'uso degli strumenti di telecomunicazione all'interno dell'istituzione o dell'organismo stesso (articolo 5, lettera a), del regolamento, convalidato dalle disposizioni di cui all'articolo 37, paragrafo 2). Tuttavia, il GEPD ha ritenuto anche che un controllo generalizzato, in contrapposizione a uno più selettivo, non sia necessario in ogni momento.

Sebbene il GEPD abbia riconosciuto la legittima finalità della gestione del bilancio, ha tuttavia ritenuto che il controllo dell'uso del telefono a fini privati, sia pure senza comunicazione dei dettagli delle chiamate effettuate, potrebbe eventualmente essere considerato una violazione del diritto alla tutela della vita privata dei dipendenti.

In proposito, il GEPD ha chiesto che l'istituzione o l'organismo assicurassero che la soglia numerica prestabilita, il cui superamento avrebbe comportato l'invio di un elenco all'amministrazione, fosse sufficientemente elevata da scongiurare controlli

ingiustificati e consentisse l'identificazione solo nei casi di abusi evidenti o ripetuti del sistema. Ha inoltre invitato l'istituzione o l'organismo a valutare in quale misura possano essere utilizzati altri indicatori per individuare eventuali abusi.

Il GEPD ha pertanto invitato l'istituzione a riconsiderare il sistema proposto e a valutare la possibilità di ricorrere ad altri metodi, meno invasivi.

2.6.7. Trattamento successivo di dati per trasferimenti all'AMEX – Autorità europea per la sicurezza alimentare

L'Autorità europea per la sicurezza alimentare (EFSA) tratta le dichiarazioni annuali d'interesse delle persone impegnate nelle sue attività, allo scopo di accertare che tali persone non abbiano conflitti d'interesse tali da interferire nelle attività che svolgono per l'EFSA.

Durante il controllo preventivo di queste operazioni di trattamento dei dati (fascicolo 2008-0737), il responsabile della protezione dei dati dell'EFSA ha chiesto la consulenza del GEPD in merito all'ulteriore utilizzo della banca dati contenente le dichiarazioni d'interesse, allo scopo di fornire alla propria agenzia viaggi (AMEX) i dati identificativi degli esperti esterni.



Il controllo dell'uso del telefono per scopi privati può essere considerato, in linea di principio, una violazione del diritto dei dipendenti alla tutela della vita privata.

Il responsabile della protezione dei dati dell'EFSA ha chiesto al GEPD se il trattamento successivo dei dati contenuti nella banca dati delle dichiarazioni d'interesse, allo scopo di fornire all'agenzia viaggi i dati identificativi degli esperti esterni, sia conforme all'articolo 4, paragrafo 1, lettera b), del regolamento.

In base alla norma citata, i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità.

Nel suo parere, il GEPD concludeva che qualsiasi trattamento successivo da parte dell'EFSA dei dati trattati nella banca dati delle dichiarazioni d'interesse, allo scopo di fornire i dati identificativi delle persone che possono beneficiare dei servizi di viaggio dell'AMEX, avrebbe avuto **finalità completamente diverse** e incompatibili con quelle iniziali della raccolta e del trattamento dei dati. Pertanto, un simile trattamento successivo da parte dell'EFSA non sarebbe stato conforme al disposto dell'articolo 4, paragrafo 1, lettera b), del regolamento.

Il GEPD ha rilevato altresì che il ruolo e le responsabilità dell'AMEX rispetto ai dati in questione non sono specificati in maniera sufficientemente chiara nell'accordo di protezione dei dati concluso tra le parti; in particolare, l'accordo non stabilisce

chiaramente per quali motivi né in quali circostanze l'AMEX funge da incaricato e/o responsabile del trattamento dei dati. È necessario attuare garanzie idonee per tutelare i diritti degli interessati e rendere sicuro il successivo trasferimento dei dati da parte dell'AMEX ad altri destinatari in conformità delle norme vigenti sulla protezione dei dati.

2.6.8. Periodi di conservazione dei documenti sanitari – Collegio dei capi dell'amministrazione

Nel novembre 2006 il presidente del Collegio dei capi dell'amministrazione (nel prosieguo "il Collegio") ha chiesto il parere del GEPD su una nota della Commissione riguardante i periodi di conservazione di alcuni documenti sanitari. Il 26 febbraio 2007 il GEPD ha adottato a tale proposito un parere nel quale sottolinea che il periodo di trent'anni indicato nella nota della Commissione non dovrebbe essere il periodo minimo di conservazione dei documenti sanitari; al contrario, fatte salve talune limitate eccezioni, esso va considerato come un periodo massimo di conservazione di tali dati. Inoltre, il GEPD ha ritenuto che l'applicazione dell'articolo 4 del regolamento comporti la necessità di esaminare la natura dei documenti sanitari al fine di stabilire il periodo di conservazione più adatto per ciascun tipo di documenti.



Il periodo di conservazione dei documenti sanitari, pari a trent'anni, va interpretato come un periodo massimo.

La questione della conservazione di documenti sanitari è stata sollevata nuovamente nel settembre 2010, quando il *Comité de Préparation pour les Affaires Sociales* (CPAS), che è la sottocommissione competente del Collegio, ha preparato una relazione su una serie di casi diversi con periodi di conservazione specifici dei documenti medici. Nell'ottobre 2010 il Collegio ha consultato il GEPD in merito a tale relazione. Il GEPD si sta occupando della questione sollevata e adotterà una posizione nella quale terrà conto del proprio parere del febbraio 2007 e della posizione espressa in precedenti pareri di controllo preventivo.

2.6.9. Norme di applicazione riguardanti il responsabile della protezione dei dati

*Il regolamento sulla protezione dei dati prevede che ciascuna istituzione o organismo dell'Unione europea adotti ulteriori **norme di applicazione concernenti i compiti, le funzioni e i poteri del responsabile della protezione dei dati.** Nel luglio 2010 il GEPD ha emesso **orientamenti** per facilitare la stesura delle norme di applicazione nei casi in cui esse non siano state ancora adottate o debbano essere riviste.*

Nel maggio 2010 l'Agenzia esecutiva del Consiglio europeo della ricerca (ERCEA) ha chiesto la consulenza del GEPD sulle proprie norme di applicazione per la funzione del responsabile della protezione dei dati. Tali norme riguardavano anche il ruolo dei controllori e le regole per l'esercizio dei diritti dei soggetti interessati. Il GEPD ha valutato favorevolmente questo approccio inclusivo, tanto più perché l'ERCEA ha accolto anche le migliori pratiche suggerite nel corso degli anni dal GEPD, quali:

- la tenuta di un inventario anonimo delle richieste scritte presentate dall'interessato per esercitare un diritto (accesso, rettifica, blocco, eccetera);
- la collaborazione con i servizi informatici e di sicurezza delle informazioni dell'Agenzia, per integrare le fonti d'informazione del responsabile della protezione dei dati.

Anche l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) e la Corte dei conti hanno consultato il GEPD in merito alla versione rivista delle rispettive norme di applicazione. Tali richieste di consulenza erano conformi agli orientamenti emessi dal GEPD.

2.7. Orientamenti tematici

L'esperienza maturata nell'applicazione del regolamento sulla protezione dei dati ha permesso al personale del GEPD di tradurre le proprie conoscenze in orientamenti generici per le istituzioni e gli organismi comunitari in materia di assunzioni, dati sanitari, indagini amministrative e procedimenti disciplinari e videosorveglianza. Il GEPD sta preparando orientamenti per la valutazione del personale e il trattamento dei dati personali nei procedimenti per molestie.

2.7.1. Orientamenti per indagini amministrative e procedimenti disciplinari

Nell'aprile 2010 il GEPD ha emesso orientamenti sul trattamento dei dati personali durante indagini amministrative e procedimenti disciplinari da parte delle istituzioni e degli organismi comunitari.

Lo scopo degli orientamenti è di armonizzare le buone pratiche in questo campo e promuovere la conformità alle disposizioni del regolamento. Gli orientamenti illustrano in modo chiaro e sintetico i risultati delle posizioni del GEPD esaminate nei pareri di controllo preventivo, e contengono anche una serie di raccomandazioni su ciascun principio fondamentale del regolamento.

Una raccomandazione importante riguarda il **diritto di accesso e rettifica** degli interessati. Questi diritti possono essere occasionalmente limitati, ma il responsabile del trattamento dei dati ha il compito di garantire che tali restrizioni siano realmente necessarie e stabilite caso per caso. Inoltre, deve assicurare che i diritti di accesso e rettifica nonché il diritto all'informazione siano garantiti con altri mezzi.

Il GEPD ha sottolineato anche la mancanza di un approccio armonizzato alla questione del **periodo di conservazione dei dati disciplinari**, in contrasto con i principi di protezione dei dati e con altri diritti fondamentali dei soggetti interessati. Tale situazione è dovuta a significative carenze nell'allegato IX allo statuto del personale, nonché alla mancanza di una politica comune delle istituzioni e degli organismi comunitari in materia di conservazione di questi dati.

Infine, il GEPD ha rilevato l'esigenza di ulteriori riflessioni sulla questione specifica delle **intercettazioni di comunicazioni**, con particolare attenzione per la base giuridica delle intercettazioni di comunicazioni orali e la possibilità di compiere tali intercettazioni senza un mandato o un'autorizzazione dell'autorità giudiziaria.

Gli orientamenti devono essere applicati dalle agenzie nelle loro notifiche al GEPD di controlli preventivi riguardanti le procedure in questo campo, ma servono anche da guida pratica per tutte le istituzioni e tutti gli organismi. Il prossimo passo del GEPD sarà la pubblicazione di un parere congiunto sulle notifiche di controllo preventivo presentate dalle agenzie alla luce degli orientamenti.

2.7.2. Orientamenti sulla videosorveglianza

Nel marzo 2010 il GEPD ha emesso una serie di orientamenti pratici per le istituzioni e gli organismi comunitari riguardo a una gestione responsabile della videosorveglianza e all'adozione di garanzie efficaci. Tali orientamenti delineano i principi di riferimento per valutare la necessità di ricorrere alla videosorveglianza e forniscono indicazioni per utilizzare la videosorveglianza in maniera tale da ridurre al minimo l'impatto sulla vita privata e su altri diritti fondamentali.

Nel luglio 2009 è stata pubblicata una bozza di consultazione, come segnalato nella relazione annuale del GEPD per il 2009. Dal processo di consultazione sono emersi riscontri per migliorare la bozza degli orientamenti e la collaborazione con le parti coinvolte.

In linea con gli orientamenti, le decisioni sull'eventuale installazione di videocamere e sul loro utilizzo non devono basarsi soltanto sulle esigenze di sicurezza, anzi, **le esigenze di sicurezza devono essere valutate alla luce dei diritti fondamentali del singolo**, senza dimenticare, però, che non necessariamente il rispetto dei diritti fondamentali è alternativo alla sicurezza. Attraverso un approccio pragmatico, fondato sui principi di selettività e proporzionalità, i sistemi di videosorveglianza possono soddisfare le esigenze di sicurezza e nel contempo rispettare la vita privata delle persone.

Entro i limiti stabiliti dalla normativa sulla protezione dei dati, ciascuna istituzione e ciascun organismo dispongono di una certa discrezionalità nella definizione dei rispettivi sistemi. Gli orientamenti hanno lo scopo di consentire la personalizzazione di questi ultimi. Tale flessibilità mira a impedire che un'interpretazione rigida o burocratica della protezione dei dati possa ostacolare il soddisfacimento di giustificate esigenze di sicurezza o il conseguimento di altri obiettivi legittimi.



Le istituzioni comunitarie hanno tempo fino al 1° gennaio 2011 per dimostrare la propria conformità alle linee direttrici del GEPD.

Nel contempo, ciascuna istituzione deve anche **dimostrare che sono in atto procedure volte a garantire la conformità** ai requisiti di protezione dei dati. Le pratiche organizzative raccomandate comprendono l'adozione di una serie di garanzie della protezione dei dati che devono essere definite nella politica di videosorveglianza dell'istituzione interessata, nonché l'esecuzione di audit periodici per accertare la conformità. Le valutazioni d'impatto compiute dalle istituzioni sono incoraggiate, mentre sarà ancora necessario richiedere controlli preventivi da parte del GEPD per le attività di videosorveglianza che comportano notevoli rischi inerenti (come la sorveglianza occulta o i sistemi complessi di sorveglianza dinamico-preventiva).

Periodo di transizione

Gli orientamenti valgono sia per i sistemi esistenti sia per quelli futuri. Le istituzioni avevano tempo fino al 1° gennaio 2011 per conformare le loro pratiche attuali. Il GEPD ha garantito la propria disponibilità ogniqualvolta c'è stato bisogno di ulteriore consulenza su questioni specifiche.

Il GEPD ha inoltre collaborato con le istituzioni che avevano già presentato le notifiche di controllo preventivo prima della pubblicazione degli orientamenti. Ci sono stati nove di questi casi, sui quali nel luglio 2010 il GEPD ha emesso raccomandazioni preliminari, con l'intesa che l'adempimento di tali raccomandazioni non esimeva l'istituzione interessata da un'approfondita analisi interna dei propri orientamenti e pratiche e della propria situazione di conformità. I commenti del GEPD avevano lo scopo di aiutare le istituzioni interessate a concentrare l'attenzione sulle questioni chiave da affrontare. Le questioni che richiedevano un'attenzione specifica erano la sorveglianza occulta e i periodi di conservazione.

Analogamente, il GEPD ha emesso anche indicazioni preliminari per l'OLAF, il cui sistema di videosorveglianza era l'unico che il GEPD aveva sottoposto a controllo preventivo prima della pubblicazione degli orientamenti (perché si trattava di una vera notifica di controllo preventivo di un sistema nuovo e, quindi, doveva essere esaminata in via prioritaria).

Il GEPD ha inoltre continuato a fornire indicazioni alle altre istituzioni sull'interpretazione e attuazione degli orientamenti, nonché a gestire i reclami e le richieste di consulenza. In tale contesto si è occupato di un reclamo contro le pratiche

di sorveglianza occulta in un'istituzione e di un'indagine amministrativa riguardante le restrizioni all'impiego come prova delle registrazioni di videosorveglianza ottenute in violazione delle norme sulla protezione dei dati.

2.8. La politica del GEPD di conformità e applicazione delle norme

Nel dicembre 2010 il GEPD ha adottato un documento politico dal titolo "Controllare e garantire la conformità al regolamento (CE) n. 45/2001".

Questa politica rappresenta un fondamentale cambio di marcia nell'applicazione del regolamento. Finora il GEPD aveva preferito emettere raccomandazioni e incoraggiare la conformità, piuttosto che mettere in guardia o ammonire i controllori o imporre disposizioni legalmente vincolanti. Ora, dopo cinque anni di una simile condotta, il GEPD ritiene che sia giunto il momento di adottare un **approccio più deciso all'applicazione delle norme**, specialmente nei casi di grave, deliberata o ripetuta mancanza di conformità ai principi della protezione dei dati. Questa politica introduce, inoltre, una serie di criteri che garantiranno un approccio proattivo e un'attuazione coerente e trasparente dei suoi poteri di applicazione delle norme.

Il documento politico delinea il quadro entro il quale il GEPD controlla, valuta e garantisce la conformità alle norme sulla protezione dei dati nell'amministrazione comunitaria, oltre a illustrare la natura dei diversi poteri di applicazione delle norme di cui è investito il GEPD e a indicare i motivi e le circostanze che possono indurlo ad adottare azioni formali.

Tale politica mira a **incoraggiare la conformità volontaria e le migliori pratiche** e a creare sufficienti incentivi per la conformità:

- evidenziando chi è responsabile della conformità;
- spiegando come il GEPD darà il proprio sostegno alla conformità;
- spiegando cosa il GEPD farà in caso di mancata conformità.

Questa politica mette altresì in rilievo il **principio della “responsabilità”** per promuovere la conformità e l’adozione di migliori pratiche all’interno dell’amministrazione dell’Unione europea. Il principio di responsabilità impone alle istituzioni e agli organismi comunitari, nonché ai controllori del trattamento di dati che sono al loro servizio, di mettere in atto misure adeguate ed efficaci al fine di garantire la conformità agli obblighi di protezione dei dati, e successivamente di provare tale conformità al GEPD.

Infine, il documento politico definisce l’approccio del GEPD alla **trasparenza e pubblicità** delle proprie attività di applicazione delle norme, sottolineando che queste qualità sono strumenti importanti sia per le parti interessate sia ai fini della buona governance. Pertanto, in futuro il GEPD pubblicherà periodicamente informazioni su tutti i deferimenti ufficiali al Parlamento, al Consiglio, alla Commissione o alla Corte di giustizia, e valuterà anche, caso per caso, l’opportunità di rendere pubbliche alcune delle sue altre attività di applicazione delle norme.

Il GEPD si augura che questo documento politico promuova un utilizzo più efficiente ed efficace delle risorse del Garante, mettendolo in condizione di concentrarsi sulle proprie responsabilità di controllo e garanzia della conformità attraverso un approccio all’applicazione delle norme che sia selettivo, mirato e basato sui rischi.



Il GEPD ritiene che sia giunto il momento per un approccio più deciso all’applicazione delle norme.

3

CONSULTAZIONE

3.1. Introduzione: panoramica degli sviluppi e delle tendenze principali

Nel 2010 la Commissione ha compiuto progressi significativi verso un **quadro giuridico** nuovo e **aggiornato della protezione dei dati in Europa**. La consultazione pubblica avviata nel 2009 si è conclusa ed è stata integrata da ulteriori consultazioni mirate con alcuni dei principali soggetti interessati.

Nel novembre 2010 la Commissione ha pubblicato una comunicazione nella quale delinea un approccio globale alla protezione dei dati personali nell'Unione europea, individuando le principali priorità e gli obiettivi chiave per la revisione delle norme attualmente vigenti.

Questo progetto è stato ai primi posti dell'agenda del GEPD nel 2010 e figurerà tra le sue priorità anche nei prossimi anni.

Nel 2010 la Commissione e il Consiglio si sono impegnati in maniera significativa per l'**attuazione del programma di Stoccolma** – un'Europa aperta e sicura al servizio e a tutela dei cittadini, approvato dal Consiglio europeo nel dicembre 2009. Il programma stabilisce gli orientamenti strategici della programmazione legislativa e operativa all'interno dello spazio di libertà, sicurezza e giustizia e si concentra sugli interessi e le esigenze dei cittadini.

Il GEPD ha controllato da vicino svariate iniziative direttamente connesse con l'attuazione del

*Il programma di Stoccolma sottolinea che le **misure di sicurezza e applicazione delle norme e il rispetto dei diritti fondamentali, compresa la protezione dei dati, devono andare di pari passo**. Riconosce altresì la necessità di proteggere i dati personali in una società globalizzata caratterizzata da una rapida evoluzione tecnologica e dallo scambio di informazioni in ambito transfrontaliero.*

programma di Stoccolma. Tra l'altro, il GEPD si è occupato di questioni fondamentali della protezione dei dati correlate alla strategia di sicurezza interna dell'UE, alla gestione delle informazioni nello spazio di libertà, sicurezza e giustizia e alla politica antiterrorismo dell'Unione europea. In linea generale, gli sviluppi legati al programma di Stoccolma sono stati i temi dominanti dell'agenda del GEPD e lo saranno anche nei prossimi anni.

Un altro punto sul quale il GEPD è intervenuto in maniera significativa è stata l'**interfaccia tra la tutela della vita privata e gli sviluppi tecnologici**. Nel maggio 2010 la Commissione ha pubblicato la comunicazione sull'agenda digitale per l'Europa, con l'obiettivo di fissare le priorità dell'Unione nel settore di Internet e delle tecnologie digitali. Molte di queste iniziative rivestono una notevole importanza per la protezione dei dati e sono strettamente monitorate dal GEPD. Il Garante è inoltre convinto del fatto che le nuove tecnologie non si limitino a porre nuove sfide per la tutela della vita privata e dei dati, ma offrano anche nuove opportunità per la protezione dei dati personali.

È dunque essenziale che i requisiti della tutela della vita privata siano integrati nella progettazione, nel funzionamento e nella gestione dei sistemi delle tecnologie informatiche e della comunicazione durante l'intero ciclo vitale dell'informazione. Il GEPD sostiene pertanto con vigore la necessità di inserire nel nuovo quadro giuridico il principio della tutela della vita privata fin dalla progettazione.

I pareri formali del GEPD, basati sull'articolo 28, paragrafo 2, o sull'articolo 41 del regolamento (CE) n. 45/2001, sono gli strumenti principali e contengono un'analisi completa di tutti gli elementi correlati alla protezione dei dati di tutte le proposte della Commissione o di altri strumenti rilevanti.

Il GEPD è stato inoltre consultato in merito a iniziative nel campo della **cooperazione internazionale per la sicurezza e l'attività di contrasto**, quali l'accordo generale tra l'Unione europea e gli Stati Uniti sulla condivisione dei dati ai fini dell'attività di contrasto e l'accordo sullo scambio di dati finanziari per le finalità del programma di controllo delle transazioni finanziarie dei terroristi (TFTP). È intervenuto anche in riferimento all'accordo commerciale anticontraffazione (ACTA) e a numerosi accordi sullo scambio dei dati dei passeggeri contenuti nel codice di prenotazione (PNR).

Il GEPD è stato attivo anche in altre aree, come gli scambi di dati su larga scala nel contesto del sistema d'informazione del mercato interno, l'utilizzo di scanner di sicurezza negli aeroporti e la cooperazione in campo fiscale.

L'ampia varietà di settori nelle quali il GEPD viene consultato è un'ulteriore dimostrazione del fatto che il trattamento dei dati sta diventando un elemento sempre più importante di un gran numero di iniziative legislative, le quali, spesso, sollevano rilevanti questioni sotto il profilo della protezione dei dati e, di conseguenza, giustificano ancora una volta il ruolo del GEPD in quanto consulente delle istituzioni comunitarie.

3.2. Quadro politico e priorità

3.2.1. Attuazione della politica di consultazione

Sebbene i metodi di lavoro del GEPD nel settore della consultazione si siano sviluppati nel corso degli anni, l'approccio di base degli interventi non è mutato. Il documento politico adottato nel marzo 2005 e intitolato "Il GEPD in quanto consulente delle istituzioni comunitarie sulle proposte legislative e sui documenti connessi" ⁽⁸⁾, pur conservando tutta la sua importanza, adesso va letto alla luce del trattato di Lisbona.

Di norma, il GEPD emette pareri su testi non legislativi (come i documenti di lavoro, le comunicazioni o le raccomandazioni della Commissione) quando la protezione dei dati è un elemento fondamentale di tali testi. Talvolta il GEPD redige commenti scritti per finalità più limitate, ad esempio per lanciare un messaggio politico veloce e fondamentale o per focalizzare l'attenzione su uno o più aspetti tecnici, o, ancora, per sintetizzare o ribadire osservazioni già fatte in precedenza.

Si possono utilizzare anche altri strumenti, come le presentazioni orali, le lettere esplicative, le conferenze stampa e i comunicati stampa. Ad esempio, nel 2010 il GEPD ha tenuto una conferenza stampa su "Il futuro del quadro giuridico dell'Unione europea per la protezione dei dati" in occasione della presentazione della relazione annuale del 2009.

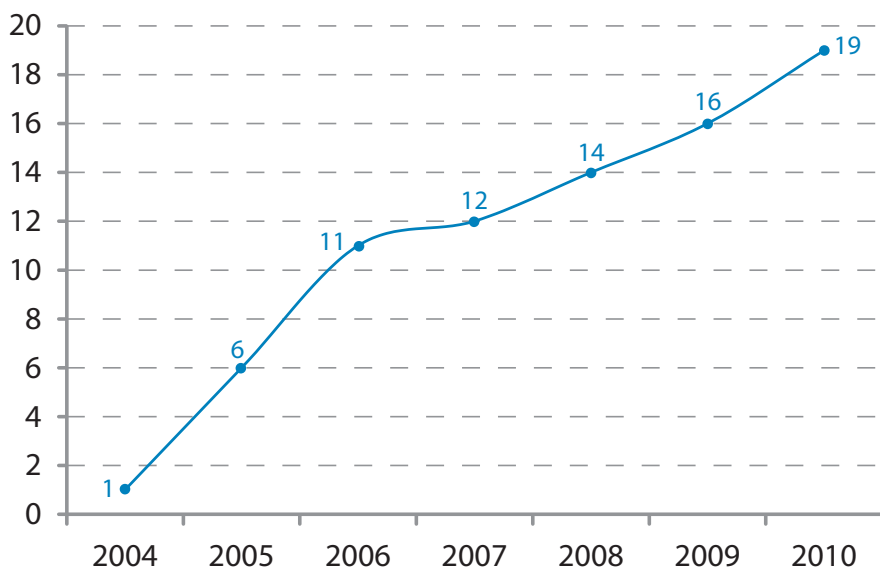
Il GEPD è disponibile durante tutte le fasi di elaborazione della politica e della legislazione e si avvale di un'ampia gamma di strumenti per svolgere le proprie funzioni di consulente. Sebbene ciò richieda talvolta uno stretto contatto con le istituzioni comunitarie, la tutela della propria indipendenza rimane una priorità assoluta.

I contatti con la Commissione avvengono in varie fasi della preparazione delle proposte; l'intensità dei contatti dipende dal tema e dall'approccio adottato dai servizi della Commissione. Questo vale in particolare per i progetti a lungo termine, quali l'iniziativa sulla giustizia elettronica e la revisione del quadro di protezione dei dati, cui il GEPD ha contribuito in varie fasi.

Il GEPD intrattiene altresì contatti regolari con i servizi delle istituzioni interessate durante la fase di follow-up. In alcuni casi, il GEPD e il suo personale sono stati coinvolti da vicino nelle discussioni e nelle trattative al Parlamento e al Consiglio; in altri casi, il principale interlocutore nella fase di follow-up è stata la Commissione. Il processo legislativo del regolamento Frontex, il seguito dato

⁽⁸⁾ Disponibile sul sito del GEPD alla voce Publications > Papers.

Andamento dei pareri legislativi 2004-2010

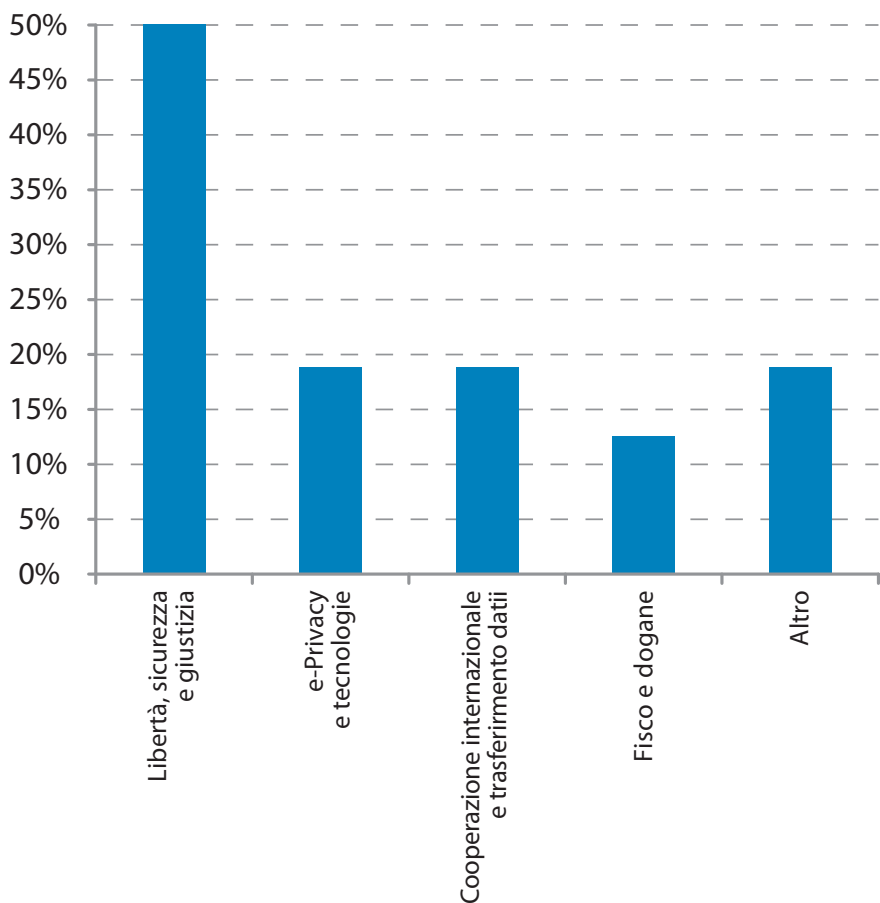


all'agenda digitale (ad esempio, la questione della neutralità della rete) e il sistema d'informazione del mercato interno sono ulteriori esempi dello stretto coinvolgimento del GEPD, che ha portato alla formulazione di altri commenti nel 2010.

3.2.2. Risultati del 2010

Il numero dei pareri ha continuato ad aumentare costantemente anche nel 2010. Il GEPD ne ha emessi 19 su una grande varietà di argomenti.

Principali aree politiche dei pareri legislativi nel 2010



Con questi pareri e con gli altri strumenti di intervento, il GEPD ha attuato le priorità stabilite per il 2010, come previsto dall'inventario. I 19 pareri hanno riguardato aree diverse della politica europea.

L'inventario del 2010 ha definito quattro aree principali su cui concentrare l'attenzione:

- il nuovo quadro giuridico per la protezione dei dati;
- libertà, sicurezza e giustizia;
- cooperazione internazionale e trasferimento di dati;
- progressi tecnologici.

Nel corso del 2010 il GEPD ha dedicato la propria attenzione in gran parte a tutte queste aree. In linea con l'inventario 2010, il GEPD si è concentrato principalmente sulle iniziative segnalate come "altamente prioritarie" in detto inventario (cioè le iniziative rosse). Il GEPD ha emesso un parere o si è attivato in altro modo riguardo a 13 delle 15 proposte altamente prioritarie adottate nel corso del 2010 ⁽⁹⁾.

Il contenuto dei pareri del GEPD e di altri contributi a titolo di consulenza è riportato di seguito in maggiore dettaglio.

3.3. Revisione del quadro comunitario di protezione dei dati

La revisione del quadro giuridico comunitario per la protezione dei dati era già stata una delle priorità principali del GEPD nel 2009, quando è iniziata ufficialmente la discussione della riforma. Nel 2010 l'interesse per la riforma è cresciuto in maniera significativa con la pubblicazione, nel novembre 2010, della comunicazione della Commissione sull'approccio globale al trasferimento dei dati personali nell'Unione europea. Il GEPD ha riservato a questo tema un'attenzione particolare durante tutto il 2010 e ha comunicato i propri messaggi in vari modi.

Il GEPD ha tenuto una **conferenza stampa** ad hoc subito dopo la pubblicazione della comunicazione,

⁽⁹⁾ In due di questi casi (revisione del regolamento (CE) n. 831/2002 relativo all'accesso ai dati riservati per fini scientifici e decisione quadro del Consiglio relativa agli attacchi contro i sistemi d'informazione) non si è ravvisata la necessità di un parere in questa fase.



Il nuovo quadro della protezione dei dati deve essere ambizioso e contribuire realmente all'efficacia degli strumenti di protezione dei dati in una società globalizzata e orientata in senso tecnologico.

per esprimere pubblicamente la propria posizione sul nuovo quadro giuridico. In quella occasione ha anche sottolineato l'importanza della revisione, che ha giudicato molto tempestiva, e ha manifestato il proprio punto di vista sugli aspetti più rilevanti del nuovo quadro.

*Il GEPD ha insistito sulla necessità di una **protezione dei dati forte ed efficace** in una società nella quale le informazioni personali sono usate in quantità incommensurabili, spesso senza che le persone ne siano consapevoli. Il GEPD ha valutato positivamente la comunicazione della Commissione, ma ha messo in guardia sul fatto che **non saranno ammessi errori**: le sfide sono enormi e le soluzioni prospettate devono essere altrettanto **ambiziose**, oltre a contribuire a una maggiore efficienza degli strumenti di protezione dei dati.*

Il GEPD ha inoltre espresso le proprie opinioni sui punti principali del nuovo quadro, sottolineando in particolare:

- il proprio sostegno al conseguimento di una **maggiore armonizzazione** delle legislazioni nazionali in materia di protezione dei dati;
- l'esigenza di un approccio **neutrale sotto il profilo tecnologico**;
- l'inclusione dei principi di **tutela della vita privata fin dalla progettazione** e di **responsabilità**;

- l'introduzione di una **notifica obbligatoria in caso di violazione della sicurezza** valida per tutti i settori pertinenti;
- l'**inclusione delle aree della polizia e della giustizia** nel quadro generale.

Il GEPD ha ulteriormente approfondito queste sue posizioni in un parere generale adottato nel gennaio 2011.

Si prevede che la Commissione adotti una proposta legislativa completa nel corso del 2011. Il GEPD continuerà a monitorare da vicino il processo legislativo anche nel 2011 e, ove opportuno, fornirà ulteriori contributi.

3.4. Spazio di libertà, sicurezza e giustizia

Nel corso del 2010 il GEPD ha seguito gli sviluppi dell'attuazione del **programma di Stoccolma** con grande attenzione e ha formulato raccomandazioni su varie iniziative legislative e non legislative direttamente o indirettamente collegate con lo spazio di libertà, sicurezza e giustizia.

3.4.1. Strategia di sicurezza interna dell'UE

La strategia di sicurezza interna dell'Unione europea (SSI) stabilisce un modello europeo di sicurezza per integrare l'attività di applicazione delle norme con la cooperazione nel settore giudiziario, la gestione dei confini e la protezione civile. All'SSI, approvata dal Consiglio nel febbraio 2010 e adottata dal Consiglio europeo un mese dopo, ha fatto seguito, nel novembre 2010, una comunicazione della Commissione in cui vengono affrontate le minacce più pressanti per la sicurezza nell'Unione europea, quali il crimine organizzato, il terrorismo, la criminalità informatica, la gestione dei confini esterni dell'UE e le catastrofi civili.

A causa della natura **potenzialmente invasiva** delle misure da adottare nel contesto della strategia, il GEPD ha seguito attentamente le discussioni sulla strategia di sicurezza interna e le azioni previste per darvi attuazione. Nel parere adottato nel dicembre 2010, il GEPD sottolinea la necessità di trovare un **giusto equilibrio** tra l'obiettivo di garantire la sicurezza dei cittadini e un'efficiente protezione della loro vita privata e dei loro dati personali. Il GEPD ha altresì sottolineato che



Il GEPD ha sollecitato la definizione di un'efficiente strategia di sicurezza interna, sostenuta e integrata da un solido sistema di protezione dei dati.

questa strategia presenta evidenti **legami politici con altre strategie comunitarie** attualmente sviluppate a livello di Unione, quali la strategia di gestione delle informazioni e la revisione del quadro giuridico comunitario della protezione dei dati.

Il GEPD ha sollecitato un **approccio più esauriente e integrato alla strategia di sicurezza interna**, tale da creare collegamenti espliciti e interazioni tra le diverse iniziative interessate. Ha sostenuto che non è possibile realizzare un'SSI efficiente senza il sostegno di un solido sistema di protezione dei dati in grado di integrarla.

3.4.2. Gestione delle informazioni

Il programma di Stoccolma ha invitato la Commissione a verificare la necessità di elaborare un **modello europeo per lo scambio di informazioni** fondato sulla valutazione degli strumenti per lo scambio di informazioni attualmente in uso. Nel programma, inoltre, si fa riferimento a un **severo regime di protezione dei dati** come prerequisito principale della strategia di gestione delle informazioni dell'Unione europea. Nel luglio 2010 la Commissione ha adottato una **comunicazione sulla revisione della gestione delle informazioni** nello spazio di libertà, sicurezza e giustizia; in proposito, il GEPD ha emesso un parere nel settembre 2010.

Inoltre, il GEPD ha proposto che, nel contesto delle attività future nel campo della gestione delle informazioni, vengano presentate relazioni e si tenga conto delle carenze e debolezze dei sistemi.

Il GEPD ha appoggiato pienamente le attività in corso mirate alla valutazione di tutti gli strumenti correlati alla gestione delle informazioni nello spazio di libertà, sicurezza e giustizia. Ha sottolineato che questa iniziativa rappresenta un **primo passo nel processo di valutazione** e ha insistito sulla necessità di una **valutazione obiettiva, esauriente e approfondita** di tutti gli strumenti attualmente disponibili nel quadro della strategia di gestione delle informazioni, prima di proporre di nuovi.

3.4.3. Frontex

Nel febbraio 2010 la Commissione ha presentato una **proposta di revisione del quadro giuridico che disciplina Frontex** al fine di potenziare le capacità operative di quella agenzia. Nel parere emesso nel maggio 2010 il GEPD si è concentrato sul numero crescente di compiti che Frontex deve svolgere e sulle loro conseguenze per la protezione dei dati.

Il GEPD ha espresso valutazioni molto negative sul fatto che la proposta non specificasse se, e se sì in quale misura, Frontex sarebbe stata autorizzata a trattare dati personali. Il GEPD ha invitato il legislatore a fissare regole chiare per la protezione dei dati e a chiarire a quali condizioni e in quali circostanze Frontex potrebbe trattare i dati.

Il GEPD ha inoltre seguito da vicino le discussioni su questo tema svoltesi nel Parlamento europeo. In una lettera indirizzata al relatore del Parlamento europeo, ha avanzato suggerimenti concreti



I dati personali correlati a sospetti non confermati di attività terroristiche non devono essere conservati a tempo indeterminato.

sull'introduzione di una **base giuridica specifica** per la questione oggetto della proposta, soggetta a **forti garanzie di protezione dei dati**, nel rispetto dei principi di proporzionalità e necessità.

3.4.4. Politica antiterrorismo

La lotta contro il terrorismo è un'area nella quale i dati personali vengono spesso trattati in maniera ampia e preventiva.

Nel suo parere sulla politica dell'Unione europea per la lotta contro il terrorismo, il GEPD ha sollecitato **iniziative concrete** a sostegno del rispetto dei diritti fondamentali in questo ambito, specialmente del diritto alla protezione dei dati personali. Il GEPD ha sottolineato l'esigenza di garantire la **coerenza** e rapporti chiari tra tutte le politiche e iniziative nel settore degli affari interni e della sicurezza interna. Ha altresì raccomandato che il legislatore comunitario **rafforzi il ruolo della protezione dei dati in quest'area**; in particolare, tutte le proposte dovrebbero considerare esplicitamente il rispetto del **principio di necessità**. Ne consegue che occorre evitare possibili sovrapposizioni con gli strumenti esistenti, mentre la raccolta e lo scambio di dati personali dovrebbe essere limitato a quanto effettivamente necessario per le finalità perseguite.

Inoltre, è auspicabile la proposta di un approccio esauriente e globale alle **misure di congelamento dei patrimoni** nei confronti di paesi specifici e di sospetti terroristi, nell'ottica di assicurare sia l'efficacia delle azioni di applicazione delle norme sia il rispetto dei diritti fondamentali. Quanto alla cooperazione internazionale, il GEPD ha richiamato l'esigenza di garantire l'adozione di garanzie appropriate negli scambi di dati personali con paesi terzi e organizzazioni internazionali, affinché i diritti dei cittadini alla protezione dei dati siano correttamente rispettati anche in quel contesto.

3.4.5. Immissione sul mercato e uso di precursori di esplosivi

Dal punto di vista della protezione dei dati, la raccolta di dati riguardanti transazioni sospette di determinate sostanze chimiche è il tema più sensibile affrontato nella proposta di regolamento della Commissione relativo all'immissione sul mercato e all'uso di precursori di esplosivi. Lo scopo principale della proposta è di ridurre il rischio di attacchi da parte di

terroristi o altri criminali per mezzo di ordigni esplosivi artigianali. Il GEPD ha chiesto che le pertinenti disposizioni siano chiarite in modo tale da assicurare che il **trattamento dei dati rimanga proporzionato e siano evitati abusi**.

Garantire un livello elevato di protezione dei dati contribuisce anche alla lotta contro il razzismo, la xenofobia e la discriminazione; a sua volta, questa lotta può contribuire alla prevenzione della radicalizzazione e del reclutamento tra le fila del terrorismo.

Le principali raccomandazioni del GEPD erano le seguenti:

- **i dati non devono essere utilizzati per finalità diverse** dalla lotta contro il terrorismo (e altri crimini che comprendono l'impiego di sostanze chimiche per la fabbricazione di ordigni esplosivi artigianali);
- **i dati non devono essere conservati per periodi di tempo prolungati**, specialmente se il numero dei destinatari effettivi o potenziali è elevato e/o se i dati devono essere utilizzati per estrapolazioni di dati. Ciò è ancora più importante nei casi in cui si può dimostrare l'infondatezza del sospetto iniziale. Il GEPD ha chiesto che il regolamento preveda un periodo massimo di conservazione (prima facie, non superiore a due anni) per tutti i dati personali riguardanti transazioni sospette segnalate;
- **il trattamento di categorie particolari di dati deve essere espressamente vietato**, per evitare pratiche discriminatorie, come l'elaborazione di profili basati sulla razza o sulla religione.

3.4.6. Regolamento Eurodac

Nel parere pubblicato nel dicembre 2010, il GEPD si è occupato del problema della **"mancata registrazione"** (che, in questo specifico contesto, significa l'impossibilità per un richiedente asilo di fornire impronte digitali leggibili). Il GEPD ha insistito sul principio secondo cui la mancata registrazione non deve comportare automaticamente la negazione dei diritti dei richiedenti asilo. In particolare, il Garante ha recisamente rigettato ogni presunzione che una persona con impronte digitali non leggibili abbia cercato – ipso facto – di vanificare la procedura di identificazione, ad esempio automutilandosi.

Nel parere citato, il GEPD ha altresì espresso la propria soddisfazione per il fatto che la **proposta attuale non contempla più** la possibilità di concedere l'**accesso a EURODAC alle autorità responsabili delle attività di contrasto**.

Il GEPD ha formulato raccomandazioni in merito all'informazione degli interessati: considerata la precaria situazione dei richiedenti asilo e degli immigrati illegali, appare ancor più necessario fornire loro informazioni accurate e utili sui loro diritti. In questo parere il GEPD si è occupato anche dell'uso delle migliori tecniche disponibili per l'attuazione del principio della tutela della vita privata fin dalla progettazione, nonché delle conseguenze della (parziale) concessione in subappalto a terzi dello sviluppo o della gestione del sistema.

Il GEPD aveva già pubblicato numerosi pareri su tali questioni. Le raccomandazioni formulate in questo parere facevano riferimento a nuovi sviluppi oppure a raccomandazioni fatte in precedenza ma non ancora recepite.

3.4.7. Abusi sessuali di minori e pedopornografia

Nel maggio 2010 il GEPD ha adottato un parere sulla proposta di direttiva della Commissione relativa alla lotta contro gli abusi sessuali e lo sfruttamento a fini sessuali di minori e contro la pedopornografia.

Nel parere il GEPD ha insistito sulla necessità di garantire la **certezza del diritto** per tutte le parti interessate, compresi i fornitori di servizi Internet (ISP), le vittime e le persone che utilizzano la rete.

Sebbene la proposta menzionasse la necessità di tener conto dei diritti fondamentali degli utenti finali, il GEPD ha ritenuto che fosse opportuno

Il GEPD non ha messo in dubbio la necessità di creare un quadro migliore per l'adozione di adeguate misure di tutela dei minori da abusi; ha però sottolineato l'**impatto** di alcune di tali misure, come il blocco dei siti Internet e la creazione di hotline, **sui diritti fondamentali alla vita privata e alla protezione dei dati** degli interessati. La questione sollevata non era legata specificamente alla lotta contro gli abusi di minori, bensì a qualsiasi iniziativa concernente la collaborazione dei privati a fini di applicazione della legge.

aggiungere alla proposta l'obbligo a carico degli Stati membri di garantire, nella lotta contro i contenuti illegali, il ricorso a **procedure armonizzate, chiare e dettagliate** sotto il **controllo di autorità pubbliche indipendenti**.

3.4.8. Ordine di protezione europeo e ordine europeo di indagine penale

Le iniziative di alcuni Stati membri in merito a una direttiva sull'ordine di protezione europeo (OPE) e sull'ordine europeo di indagine penale (OEIP) rientrano nel contesto del programma di Stoccolma e prevedono lo scambio di dati personali tra gli Stati membri interessati. Mentre l'OPE ha lo scopo di migliorare la tutela delle vittime di crimini (in particolare le donne), l'OEIP mira a creare uno strumento unico, efficiente e flessibile per ottenere prove che si trovano in un altro Stato membro dell'Unione europea.

Nel suo parere il GEPD ha sottolineato che il trattamento di dati personali, specialmente in un'area sensibile come lo spazio di libertà, sicurezza e giustizia, deve essere conforme alla legislazione comunitaria in materia di protezione dei dati.

Una protezione efficace dei dati personali non soltanto è importante per gli interessati, ma contribuisce anche al successo della cooperazione in campo giudiziario perché rafforza la collaborazione fondata sul riconoscimento reciproco e una migliore qualità dei dati nello scambio di informazioni.

Tra le varie raccomandazioni formulate, il GEPD ha sollecitato l'adozione di garanzie appropriate per tutelare le persone durante il trattamento dei dati personali e per assicurare la correttezza delle procedure e il rispetto delle norme sulla riservatezza e il segreto professionale. Più in particolare, il GEPD ha sottolineato l'esigenza di garantire che, primo, i sistemi di autenticazione consentano l'accesso ai dati personali solamente alle persone autorizzate; secondo, che sia eseguito il tracciamento degli accessi; terzo, che siano attuati controlli di audit.

Questo parere, inoltre, ha offerto al GEPD un'importante occasione per evidenziare anche la necessità di introdurre **procedure specifiche** per garantire la **consultazione del Garante anche** nei casi in cui un'iniziativa adottata da uno Stato membro riguardi il trattamento di dati personali.

3.5. e-Privacy e tecnologia

3.5.1. Promuovere la fiducia nella società dell'informazione

Nel maggio 2010 la Commissione europea ha adottato l'agenda digitale, una strategia che comprende una serie di politiche e azioni per stimolare l'economia digitale entro il 2020. Come contributo a tale strategia, nel marzo 2010 il GEPD aveva adottato un parere sulla promozione della fiducia nella società dell'informazione attraverso l'incentivazione della protezione dei dati e della vita privata.

Nel parere si evidenzia come la fiducia dei consumatori costituisca un fattore decisivo della diffusione e di un efficace impiego delle tecnologie dell'informazione e della comunicazione (TIC), delle quali l'identificazione a radio frequenza, le reti sociali, la sanità elettronica e i trasporti elettronici sono solo alcuni esempi.

La fiducia si può creare soltanto se le TIC sono affidabili, sicure e sotto il controllo delle persone interessate, e se è garantita la protezione dei dati personali e della vita privata.

L'Unione europea può vantare un robusto quadro normativo in materia di protezione dei dati che, in linea di principio, dovrebbe assicurare la protezione dei dati personali dei cittadini. In molti casi, però, le TIC suscitano nuovi timori, non contemplati nel quadro esistente. Il parere prendeva in esame le misure che possono essere discusse o promosse dall'Unione europea per potenziare questo quadro. In particolare, il GEPD ha invitato la Commissione europea a fare quanto segue:

- integrare il principio di **tutela della vita privata fin dalla progettazione**, come **principio vincolante di validità generale**, nel quadro giuridico vigente in materia di protezione dei dati. Tale principio, inoltre, dovrebbe essere pienamente recepito nell'agenda digitale europea e diventare un principio vincolante delle politiche comunitarie future, ad esempio nel campo del trasporto elettronico, del governo elettronico, eccetera;
- dare attuazione al principio della tutela della vita privata fin dalla progettazione seguendo uno specifico approccio in tre **aree delle TIC che comportano rischi specifici** per la protezione

della vita privata e dei dati: a) **identificazione a radiofrequenza (RFID)**: proporre misure legislative per disciplinare gli aspetti più importanti dell'uso dell'identificazione a radiofrequenza laddove l'autoregolamentazione non dia i risultati sperati (ad esempio, garantire il principio di poter aderire a questo servizio nel punto vendita); b) **reti sociali**: stabilire l'obbligatorietà di impostazioni predefinite di tutela della vita privata; c) **pubblicità mirata**: prevedere che i motori di ricerca siano dotati di impostazioni predefinite di tutela della vita privata per facilitare l'ottenimento del consenso a ricevere pubblicità.

3.5.2. Internet e neutralità della rete

Nel giugno 2010 la DG Società dell'informazione e mezzi di comunicazione (INFSO) ha avviato una consultazione pubblica sull'Internet aperta e sulla neutralità della rete in Europa. Nella consultazione sono state proposte una serie di domande relative alle politiche di gestione del traffico che consentono agli operatori della rete e ai fornitori di servizi Internet di gestire il traffico in maniera particolare.

In risposta alla consultazione, il GEPD ha formulato commenti volti a segnalare alla DG INFSO le questioni connesse con la protezione dei dati e della vita privata che sorgono quando i fornitori di servizi Internet e gli operatori della rete attuano pratiche di gestione del traffico.

Il GEPD ha messo in evidenza due aspetti correlati all'attuazione dei meccanismi di gestione del

traffico: primo, questi meccanismi consentono ai fornitori di servizi Internet di vedere il contenuto di messaggi o trasmissioni e, secondo, danno loro la possibilità di attribuire tali contenuti a un determinato utente. Il GEPD ha sottolineato l'esigenza di tenere in debita considerazione il quadro normativo comunitario in materia di protezione dei dati quando si compiono azioni del genere. Più nello specifico, il Garante ha fatto presente che il quadro comunitario di protezione dei dati obbliga gli utenti a ottenere un **consenso libero e informato**, e ha fornito orientamenti pratici sui requisiti per il suo ottenimento.

3.5.3. Direttiva sulla conservazione dei dati

A una conferenza organizzata dalla Commissione nel dicembre 2010, il GEPD ha tenuto un discorso – riguardante il “momento della verità” per la direttiva sulla conservazione dei dati – nel quale ha sostenuto che era doveroso cogliere l'occasione per **dimostrare chiaramente** che la direttiva **era necessaria e giustificata**.

Questa direttiva comporta l'obbligo per i fornitori di comunicazioni elettroniche pubbliche (aziende telefoniche, fornitori di servizi di telecomunicazione mobili e di servizi Internet) di conservare i dati relativi al traffico, all'ubicazione e all'abbonato a fini di indagine, accertamento e perseguimento di reati gravi.



Il GEPD ha invitato la Commissione a dimostrare la necessità di conservare una così grande quantità di dati riguardanti comunicazioni.

Il GEPD ha sottolineato che un'invasione così massiccia della vita privata necessitava di una giustificazione molto valida e ha pertanto invitato la Commissione europea a compiere un esercizio di valutazione per **dimostrare la necessità** della direttiva in parola attraverso fatti e cifre concreti, al fine di accertare se i risultati presentati nella valutazione si sarebbero potuti conseguire con mezzi diversi, meno invasivi.

Uno strumento comunitario nuovo o modificato per la conservazione dei dati deve indicare con chiarezza le proprie finalità e fornire ai cittadini la certezza del diritto. Ciò significa che deve anche regolamentare le opportunità di accesso e uso successivo da parte delle autorità preposte all'applicazione della legge, senza lasciare agli Stati membri margini per l'utilizzo dei dati per finalità aggiuntive.

Sentenza della Corte costituzionale tedesca

Il 2 marzo 2010 la Corte costituzionale tedesca ha emesso una sentenza **contro la legge tedesca che recepisce la direttiva sulla conservazione dei dati**. La Corte ha stabilito che l'uso dei dati conservati doveva essere sottoposto a requisiti più severi di quelli previsti dal legislatore tedesco. Nella sua valutazione, la Corte ha quindi formulato criteri più restrittivi per l'accesso ai dati e per il loro utilizzo. Tali criteri dovranno essere inseriti nella legislazione nazionale tedesca al fine di garantire che l'obbligo di conservazione dei dati possa essere adempiuto senza che siano violati i diritti fondamentali sanciti dalla costituzione tedesca.

In una dichiarazione alla stampa, il GEPD ha sottolineato che quella sentenza va vista come una fonte autorevole di ispirazione per gli altri Stati membri dell'Unione europea nonché come un prezioso contributo alla valutazione della direttiva sulla conservazione dei dati, specialmente alla luce del nuovo quadro giuridico istituito con il trattato di Lisbona.

3.5.4. Rifiuti elettronici

La protezione della vita privata e dei dati è intrinsecamente legata alle misure concernenti i dispositivi in grado di memorizzare una quantità crescente di dati personali. Il GEPD ha evidenziato questo aspetto nel proprio parere dell'aprile 2010

sulla proposta della Commissione di rifusione della direttiva sui rifiuti di apparecchiature elettriche ed elettroniche (o più semplicemente rifiuti elettronici).

Pur condividendo l'obiettivo della proposta, cioè migliorare le politiche ecocompatibili nel settore dei rifiuti elettronici, il GEPD ha tuttavia fatto presente che l'iniziativa riguardava soltanto i rischi ambientali correlati allo smaltimento dei rifiuti elettronici e non prendeva in considerazione i **rischi per la protezione dei dati** che possono derivare da uno **smaltimento, riutilizzo o riciclaggio inadeguati** dei rifiuti elettrici ed elettronici.

Sussiste un maggior rischio di perdita e dispersione di dati personali quando i dati personali dell'utilizzatore delle apparecchiature e/o di soggetti terzi sono ancora immagazzinati nelle apparecchiature informatiche e di telecomunicazione (ad esempio, personal computer, computer portatili e dispositivi di comunicazione elettronici) al momento dello smaltimento.

Alla luce di questi rischi, il GEPD ha sottolineato l'importanza di adottare idonee **misure di sicurezza** in ogni fase del trattamento dei dati personali, anche durante lo smaltimento delle apparecchiature contenenti dati personali (dall'inizio alla fine).



I dati personali memorizzati nei rifiuti elettronici devono essere protetti in modo adeguato.

Inoltre, vanno tenuti nel debito conto il **principio della tutela della vita privata fin dalla progettazione** e, in tale ambito, il principio di **sicurezza fin dalla progettazione**, i quali devono essere contemplati nella proposta al fine di garantire che la tutela della vita privata e della sicurezza sia integrata come impostazione predefinita nella progettazione di apparecchiature elettriche ed elettroniche.

3.5.5. Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

In un parere pubblicato nel dicembre 2010 il GEPD ha accolto con favore l'estensione del mandato dell'ENISA e l'ampliamento dei suoi compiti attuali, come proposto dalla Commissione europea, e ha sottolineato che la **sicurezza del trattamento dei dati** costituisce un **elemento essenziale della loro protezione**. In proposito, il Garante ha dichiarato di condividere l'obiettivo della proposta di potenziare le competenze dell'Agenzia inserendovi come **parti interessate a pieno titolo** le **autorità responsabili della protezione dei dati** e gli **organi preposti all'applicazione della legge**.

Il GEPD ha raccomandato di precisare meglio la questione dell'ampliamento dei compiti dell'Agenzia, per evitare una situazione di incertezza giuridica, e di stabilire solidi canali di cooperazione con le parti interessate dell'Agenzia, per garantire coerenza e una stretta collaborazione.

Il GEPD ha altresì sottolineato la necessità di integrare le **raccomandazioni sulla sicurezza e le migliori pratiche** nelle operazioni interne dell'Agenzia. In tal modo l'ENISA potrà sperimentare meglio e promuovere queste tecniche presso altri organismi e altre agenzie.



Il nuovo regolamento dell'ENISA estenderà il mandato dell'agenzia di cinque anni e ne rafforzerà le competenze.

3.5.6. Giustizia elettronica

Il GEPD sta collaborando strettamente con i gruppi della Commissione e del Consiglio impegnati a dare avvio e attuazione al piano d'azione in materia di giustizia elettronica. Questa iniziativa è tesa ad ammodernare e ottimizzare il modo in cui le persone ricevono informazioni attinenti all'amministrazione della giustizia, affinché possano beneficiare di uno "sportello unico multilingue online per l'informazione in campo giudiziario".

Il portale è stato inaugurato nel luglio 2009 con una funzionalità ridotta e dovrebbe incorporare altri servizi, secondo l'ambizioso programma predisposto dal Consiglio, che prevede anche altre funzioni: servizi informativi, pagamenti elettronici, un ordine europeo per la procedura di pagamento, piccoli reclami, ricerca di professionisti, ricerca di informazioni in registri pubblici interconnessi.

Poiché alcuni di questi servizi comportano probabilmente il trattamento di quantità notevoli di dati personali, il GEPD ha raccomandato di inserire sin dall'inizio appropriate **garanzie per la protezione dei dati** negli strumenti giuridici che costituiscono la base giuridica nonché nell'infrastruttura informatica che fornisce tali servizi.

3.5.7. Settimo programma quadro di RST, compreso il progetto Turbine

Applicando le possibili opzioni di interazione indicate nel suo documento politico dell'aprile 2008 intitolato "Il Garante europeo della protezione dei dati e la ricerca e lo sviluppo tecnologico dell'Unione europea" ⁽¹⁰⁾, nel 2010 il GEPD ha favorito l'avvio di contatti e collaborazioni tra le autorità nazionali responsabili della protezione dei dati e i consorzi di progetti di ricerca.

Il caso di Turbine ⁽¹¹⁾

Nel 2008, dopo aver esaminato gli elementi del progetto comunitario "TrUsted Revocable Biometric IdeNtitiEs" (Turbine), mirato all'esecuzione di ricerche nel campo delle **identità biometriche revocabili**, il GEPD ha deciso di rispondere favorevolmente alla richiesta di un parere su tale progetto avanzata dal consorzio di ricerca ⁽¹²⁾. Il GEPD ha

⁽¹⁰⁾ Disponibile sul sito del GEPD alla voce Publications > Papers.

⁽¹¹⁾ www.turbine-project.eu

⁽¹²⁾ Cfr. relazione annuale 2008, pag. 70.

espresso apprezzamento per la rilevanza attribuita dal progetto alle questioni della protezione dei dati, ritenendo che ciò fosse in linea con le priorità individuate nella propria relazione annuale.

Tra maggio e ottobre 2010 il consorzio di progetto ha messo a disposizione del GEPD tutta la documentazione pertinente relativa agli aspetti della protezione dei dati nella ricerca condotta nell'ambito del progetto Turbine. Il GEPD ha inoltre avuto numerose discussioni con rappresentanti del consorzio, per ottenere ulteriori chiarimenti e, ove richiesta, ha ottenuto anche ulteriore documentazione. I dimostratori sviluppati da Turbine e messi in funzione nell'estate del 2010 sono stati considerati un importante elemento di analisi. I punti salienti del parere del Garante sono stati presentati in occasione della conferenza conclusiva del progetto, svoltasi a Bruxelles nel gennaio 2011.



Il settimo programma quadro è il punto di partenza per la tutela della vita privata fin dalla progettazione.

3.6. Cooperazione internazionale e trasferimenti di dati

3.6.1. Dati dei passeggeri contenuti nel codice di prenotazione

Nel 2010, come già negli anni precedenti, il trattamento dei dati dei passeggeri contenuti nel codice di prenotazione (PNR) da parte delle autorità preposte all'applicazione della legge ha sollevato alcune problematiche connesse con la protezione dei dati in una prospettiva europea.

In merito all'**accordo con gli Stati Uniti sui dati del codice di prenotazione**, il GEPD ha ribadito alcune perplessità che aveva già sollevato nei propri interventi di fronte alla Corte di giustizia e nei pareri adottati insieme con il gruppo di lavoro Articolo 29, ma che non avevano trovato sufficiente attenzione nella versione definitiva dell'accordo. In particolare, il GEPD ha sottolineato che l'accordo non si limita a riguardare le persone che possono comportare rischi, bensì prevede la raccolta massiccia di dati personali e la valutazione del rischio applicata a tutti i passeggeri. L'accordo sui dati del codice di prenotazione concluso con l'Australia ha invece sollevato minori preoccupazioni sotto il profilo della tutela della vita privata.

Il GEPD ha anche preso posizione sulla proposta della Commissione di **definizione della sua strategia esterna in materia di PNR**. La proposta delinea i principi generali, tra cui una serie di standard per la protezione dei dati, sui quali devono fondarsi tutti gli accordi relativi ai dati del codice di prenotazione conclusi con paesi terzi. Nel parere, il GEPD ha apprezzato l'approccio orizzontale seguito dalla Commissione e ha espresso il proprio fermo sostegno per l'obiettivo di realizzare una protezione dei dati armonizzata e di alto livello in tutti i sistemi PNR esistenti e futuri.

Tuttavia, per essere accettabili, le condizioni per la raccolta e il trattamento dei dati del codice di prenotazione vanno **notevolmente limitate**. Come nel caso dell'accordo PNR con gli Stati Uniti, il GEPD ha espresso preoccupazione circa il possibile **utilizzo dei sistemi PNR a fini di valutazione del rischio o di elaborazione di profili**. Ha manifestato gravi timori quanto alla **necessità e liceità** di alcuni aspetti importanti dei sistemi proposti. A suo parere, un utilizzo attivo dei dati del codice di prenotazione di tutti i passeggeri per la valutazione del rischio richiede giustificazioni e garanzie più esplicite.

Per quanto attiene al contenuto degli standard proposti per la protezione dei dati, il GEPD ha sollecitato una maggiore precisione delle **garanzie minime** applicabili a tutti gli accordi PNR. In particolare, devono essere previste condizioni più severe per il trattamento dei dati sensibili, i trasferimenti successivi dei dati e la loro conservazione. Il GEPD ha altresì sottolineato la necessità che tutti gli accordi PNR prevedano esplicitamente **diritti immediatamente applicabili** per i cittadini.



I dati personali di tutti i passeggeri sono utilizzati a fini di valutazione del rischio. Tale uso solleva gravi questioni di necessità e proporzionalità.

3.6.2. Programma di controllo delle transazioni finanziarie dei terroristi

Il GEPD ha manifestato significativa preoccupazione in merito all'accordo quadro della Commissione europea con gli Stati Uniti sul **programma di controllo delle transazioni finanziarie dei terroristi (TFTP)**, in forza del quale le autorità statunitensi, nell'ambito di indagini contro il terrorismo, possono accedere ai dati finanziari conservati in Europa e gestiti dalla società belga **SWIFT**. A seguito della decisione adottata dal Parlamento europeo a metà febbraio di porre il veto sull'accordo provvisorio, è stata redatta una nuova versione dell'accordo per tener conto dei dubbi concernenti la protezione della vita privata e dei dati.

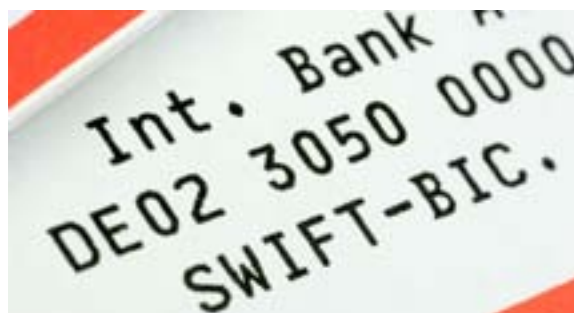
*Il GEPD ha ritenuto che **non erano state fornite prove sufficienti a giustificare la necessità e la proporzionalità** di un accordo dagli effetti così invasivi per la vita privata e che, sotto molti aspetti, costituiva un doppione rispetto a strumenti comunitari e internazionali già esistenti in materia.*

Il GEPD ha sottolineato che la **necessità** dell'accordo proposto doveva essere accertata senz'ombra di dubbio, prendendo in considerazione gli strumenti già disponibili e meno invasivi della vita privata (ad esempio, l'accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti), e ha espresso particolari preoccupazioni sul progetto di autorizzare il **trasferimento di quantità massicce di dati bancari** alle autorità statunitensi (trasferimenti in massa).

Inoltre, nel suo parere il GEPD ha indicato gli interventi da attuare per migliorare gli aspetti rilevanti dal punto di vista della protezione dei dati, tra cui:

- garantire che i **trasferimenti in massa** siano sostituiti da meccanismi che permettono di filtrare i dati finanziari nell'Unione europea, in modo tale da inviare alle autorità statunitensi soltanto i dati pertinenti e necessari;
- ridurre considerevolmente il **periodo di conservazione** dei dati non estratti ai quali le autorità non hanno avuto accesso a fini di indagini antiterrorismo;
- affidare a un'**autorità giudiziaria pubblica** il compito di esaminare le richieste del ministero del Tesoro degli Stati Uniti, conformemente al mandato negoziale e al quadro giuridico comunitario vigente in materia di protezione dei dati;
- garantire che i **diritti alla protezione dei dati** degli interessati possano essere **effettivamente esercitati**, specialmente nel territorio statunitense;
- rafforzare il **controllo indipendente e i meccanismi di vigilanza**.

Alcuni di questi interventi sono stati discussi dalla Commissione europea, dal Parlamento europeo e dal Consiglio durante la procedura finale. Un accordo leggermente rivisto è entrato in vigore il 1° agosto 2010.



Il GEPD ha manifestato le proprie perplessità riguardo al progetto di consentire trasferimenti massicci di dati bancari alle autorità degli Stati Uniti.

3.6.3. Accordo internazionale UE-USA sulla condivisione delle informazioni e la protezione dei dati personali

Il GEPD contribuisce alle discussioni per la stesura di un accordo internazionale sulla protezione dei dati tra l'Unione europea e gli Stati Uniti che dovrebbe

fornire **garanzie di alto livello** per gli scambi di dati personali nel settore della **cooperazione di polizia e giudiziaria in materia penale**.

Dal 2007 il GEPD segue da vicino l'attività del gruppo di contatto di alto livello, formato da rappresentanti dell'Unione europea e degli Stati Uniti, e ha contribuito attivamente alle diverse fasi dei lavori preparatori. Ha emesso un parere, nel novembre 2008, e ha partecipato alle riunioni e alla consultazione pubblica organizzata dalla Commissione. Riguardo al mandato negoziale predisposto dalla Commissione, il GEPD ha appoggiato l'inserimento nella bozza dell'accordo dei requisiti essenziali per la protezione dei dati, quali una chiara definizione delle finalità e dell'ambito di applicazione dell'accordo, norme sui diritti che gli interessati possono esercitare e una vigilanza indipendente.

3.6.4. Accordo commerciale anticontraffazione

Durante tutto il 2010 l'Unione europea è stata impegnata in trattative sulla conclusione di un accordo commerciale internazionale anticontraffazione (ACTA). Tale accordo, adottato nel dicembre 2010, ha lo scopo di rafforzare l'applicazione dei diritti di proprietà intellettuale, anche in Internet.

*Il GEPD, che non era mai stato consultato prima su questo tema, era particolarmente preoccupato per le disposizioni dell'accordo che avrebbero potuto legittimare un **controllo su larga scala degli utenti di Internet** e che obbligavano i fornitori di servizi Internet ad adottare **"politiche di disconnessione da Internet dopo tre avvisi"** ⁽¹³⁾.*

Nel corso delle trattative, che sono state pesantemente criticate a causa della mancanza di trasparenza, è emerso che talune disposizioni della bozza di accordo potevano costituire una violazione dei diritti delle persone alla protezione della vita privata e dei dati personali.

Questi dubbi sono stati oggetto di un parere adottato dal GEPD nel febbraio 2010 che conteneva anche le seguenti raccomandazioni:

- **valutare la possibilità di avvalersi di mezzi meno invasivi per contrastare la pirateria in Internet:** il GEPD ha sostenuto che le politiche basate sull'approccio dei tre avvisi non sono necessarie per conseguire l'obiettivo di rafforzare

⁽¹³⁾ Tali politiche comportano di prassi l'annullamento della connessione a Internet dopo che l'utente è stato messo in guardia da presunte attività illegali di condivisione o scaricamento di materiale protetto da copyright.



Il GEPD ha manifestato perplessità con riguardo alle disposizioni dell'ACTA che sembrano legittimare un controllo su larga scala degli utenti di Internet.

i diritti di proprietà intellettuale e ha chiesto che fossero prese in considerazione soluzioni meno invasive o che, quanto meno, fosse limitato l'ambito di applicazione previsto per i controlli, privilegiando un monitoraggio mirato ad hoc;

- **adottare garanzie appropriate per tutti i trasferimenti di dati nel contesto di ACTA:** nella misura in cui ACTA comporti scambi internazionali di dati personali tra autorità e/o organizzazioni private con sede nei paesi firmatari, il GEPD ha invitato l'Unione europea ad adottare garanzie appropriate per tutti i trasferimenti di dati effettuati nel contesto dell'accordo. Tali garanzie dovrebbero consistere in accordi vincolanti tra i mittenti dei dati nell'Unione europea e i destinatari in paesi terzi.

3.7. Fiscalità e dogane

3.7.1. Cooperazione nel settore fiscale

Il primo parere emesso dal GEPD nel 2010 ha riguardato la proposta della Commissione sul rafforzamento della cooperazione amministrativa tra gli Stati membri nel settore fiscale. La proposta affrontava la tassazione indiretta ma non l'IVA né le imposte sui consumi che sono trattate in altri strumenti giuridici.

Uno degli scopi principali della proposta era di migliorare lo scambio di informazioni tra gli Stati membri. Nella maggior parte dei casi, lo scambio aveva per oggetto informazioni su persone fisiche e, quindi, era soggetto alle norme sulla protezione dei dati.

In questo parere del gennaio 2010, il GEPD ha rilevato che la proposta della Commissione costituiva un chiaro esempio di **mancaza di consapevolezza della protezione dei dati** perché la questione della protezione dei dati era stata quasi completamente ignorata e per tale motivo la proposta conteneva numerosi elementi, illustrati e discussi nel parere, non conformi ai requisiti della protezione dei dati.

Tra le altre osservazioni, il GEPD ha invitato il legislatore a definire con maggiore chiarezza la responsabilità della Commissione per la **manutenzione e sicurezza della rete** da utilizzare per lo scambio di informazioni. Inoltre, ha chiesto al legislatore di specificare il tipo di informazioni personali che potevano essere scambiate, di meglio definire le

finalità per le quali fosse ammesso lo scambio di dati personali e di valutare la necessità dei trasferimenti di dati, o quanto meno di garantire il rispetto del principio di necessità.

3.7.2. Cooperazione doganale UE-Giappone

Nel febbraio 2010 la Commissione ha adottato una proposta di decisione del Consiglio relativa alla posizione dell'Unione in seno al Comitato misto di cooperazione doganale UE-Giappone in materia di riconoscimento reciproco dei programmi di operatore economico autorizzato nell'Unione europea e in Giappone⁽¹⁴⁾. L'articolo IV dell'allegato alla proposta riguarda lo **scambio di informazioni e la comunicazione** e prevede che le informazioni e i relativi dati, riguardanti in particolare gli aderenti ai programmi, siano trasmessi sistematicamente in formato elettronico.

Sia la direttiva 95/46/CE che il regolamento (CE) n. 45/2001 contengono disposizioni analoghe in materia di flussi transfrontalieri di dati personali, rispettivamente negli articoli 25-26 della direttiva e nell'articolo 9 del regolamento. Il principio sancito in tali articoli stabilisce che i **dati personali non possano essere trasferiti** da uno Stato membro a un paese terzo **a meno che** il paese terzo garantisca un **adeguato livello di protezione** (a meno che siano adottate garanzie appropriate, oppure trovi applicazione una delle eccezioni previste).

Sebbene la bozza di relazione della proposta dichiarasse che il sistema di protezione dei dati giapponese era appropriato, nel caso di specie la procedura prevista dalla direttiva per l'accertamento dell'esistenza, nel paese terzo considerato, di un adeguato livello di protezione non era stata rispettata. Di conseguenza, la dichiarazione contenuta nella relazione costituiva una violazione della direttiva.

Il GEPD ha raccomandato quindi che fosse depennata la dichiarazione di adeguatezza del sistema giapponese riportata nel punto 5, paragrafo 1, della bozza di memorandum esplicativo, in quanto non conforme ai requisiti del regolamento (CE) n. 45/2001 e della direttiva 95/46/CE, e che fossero esaminate altre possibilità, in linea con il regolamento e la direttiva, per garantire il rispetto delle norme sui trasferimenti internazionali.

⁽¹⁴⁾ COM(2010) 55 definitivo.

3.8. Accesso del pubblico, inclusi i procedimenti giurisdizionali relativi

3.8.1. Accesso del pubblico a documenti contenenti dati personali

Sin dall'inizio della sua attività, il GEPD si è costantemente occupato del rapporto, talvolta controverso, tra le norme comunitarie sull'**accesso del pubblico a documenti** e le norme comunitarie sulla **protezione dei dati**. Lo ha fatto dapprima fornendo orientamenti alle istituzioni dell'Unione europea, ad esempio nel 2005 con la pubblicazione del documento quadro intitolato "Accesso del pubblico ai documenti e protezione dei dati", contenente orientamenti per le istituzioni e gli organismi dell'Unione europea.

Successivamente il GEPD ha difeso il proprio approccio in qualità di interveniente nella causa tra la Bavarian Lager e la Commissione. Tale procedimento verteva sulla richiesta di accesso ai verbali di una seduta della Commissione e all'elenco dei partecipanti. L'accesso a quei nomi era stato negato in virtù delle norme sulla protezione dei dati. Mentre il Tribunale aveva concordato con la posizione sostenuta dal GEPD, la Corte di giustizia, nella sua sentenza di appello del 29 giugno 2010, revocava la decisione del Tribunale e dava una diversa interpretazione delle norme comunitarie applicabili al caso in esame.

Una parte dell'analisi presentata nel documento di inquadramento del 2005 ora non è più valida per effetto della decisione della Corte. Pertanto il GEPD ha redatto su questa materia un breve documento integrativo che è stato ultimato e pubblicato nei primi mesi del 2011.

Nel documento aggiuntivo il GEPD rileva la necessità di un **approccio proattivo** alla questione. Ciò significa, in sintesi, che le istituzioni devono spiegare chiaramente agli interessati – prima o al più tardi al momento della raccolta dei dati personali – in quale misura il trattamento dei loro dati comporti o possa comportare la rivelazione dei dati stessi al pubblico. Il GEPD ha sostenuto che le istituzioni hanno l'obbligo di comportarsi in questo modo a titolo di buona pratica.

Un approccio proattivo riduce il numero dei casi nei quali le istituzioni devono decidere l'eventuale rivelazione pubblica di dati a seguito di una richiesta di accesso da parte del pubblico, come nella causa della Bavarian Lager. Il documento fornisce consigli su come trovare un giusto equilibrio sia in situazioni proattive che in situazioni reattive.

Molti processi pendenti sono stati sospesi in attesa della decisione nella causa Bavarian Lager e sono poi ripresi tutti dopo la sentenza emessa dalla Corte nel giugno 2010. Il GEPD ha partecipato a molti di quei procedimenti in qualità di interveniente. Ove opportuno, il GEPD ha colto l'occasione per esprimere la propria opinione sull'applicazione agli altri procedimenti della sentenza nella causa Bavarian Lager. Il GEPD ha altresì dato un contributo in questo senso a un nuovo procedimento avviato su tale questione.

Una delle conseguenze della sentenza nella causa Bavarian Lager è stata l'archiviazione del primo procedimento promosso contro il GEPD dinanzi alla Corte generale.

3.8.2. Altri procedimenti giudiziari

Un'altra sentenza che ha visto il coinvolgimento del GEPD è stata quella emessa dal Tribunale della funzione pubblica il 15 giugno 2010 nella causa tra la Pachtitis e la Commissione europea. Tra i punti dibattuti c'era il rifiuto della Commissione di concedere al ricorrente l'accesso alle domande di un test di assunzione al quale egli aveva partecipato. Poiché erano state citate le norme sulla protezione dei dati, e la questione sollevava un interrogativo interessante sull'ambito di applicazione del diritto di accesso ai propri dati personali, il GEPD ha deciso di intervenire e lo ha fatto appoggiando le richieste del ricorrente. Questi ha vinto la causa, però la questione della protezione dei dati non è stata affrontata. Per tale ragione, il GEPD si è ritirato dal successivo procedimento di appello promosso dalla Commissione davanti al Tribunale.

Nel luglio 2010 il Tribunale della funzione pubblica ha invitato il GEPD a intervenire in una causa riguardante il trasferimento di dati sanitari tra due istituzioni comunitarie. Quella è stata la prima volta che la Corte ha sollecitato l'intervento del GEPD in un procedimento. Il GEPD ha accolto l'invito e redatto una memoria d'intervento nella quale ha precisato le disposizioni pertinenti del regolamento sulla protezione dei dati.

3.9. Altre questioni

3.9.1. Sistema d'informazione del mercato interno

Nel luglio 2010 il GEPD ha inviato una lettera alla direzione generale Mercato interno e servizi della Commissione (DG MARKT) nella quale faceva il bilancio di quanto era stato ottenuto e quanto restava ancora da fare sulle questioni sollevate nella relazione della Commissione concernente la situazione della protezione dei dati nel sistema d'informazione del mercato interno (IMI).

L'IMI è un'applicazione online che permette agli Stati membri di collaborare tra loro per migliorare l'applicazione della normativa sul mercato interno. In tale contesto, vengono tra l'altro registrati e condivisi dati personali rilevanti. In particolare, l'IMI consente alle autorità nazionali, regionali e locali degli Stati membri dell'Unione europea di comunicare rapidamente e facilmente con i loro omologhi in altri paesi europei. Il sistema aiuta gli utenti a individuare l'autorità da contattare in un altro paese e a comunicare con essa usando una serie di domande e risposte pre-stabilite già tradotte. L'IMI è un sistema flessibile che può essere utilizzato per molte disposizioni della legislazione sul mercato interno.

Il GEPD ha valutato positivamente i progressi compiuti finora e ha incoraggiato la Commissione a mettere in atto **ulteriori garanzie**, in applicazione del principio di **tutela della vita privata fin dalla progettazione**, nonché a proseguire, ove necessario, la cooperazione con le autorità di protezione dei dati negli Stati membri. È importante rilevare anche che il GEPD ha invitato la Commissione ad adottare un nuovo strumento giuridico, preferibilmente nell'ambito della procedura legislativa ordinaria, per istituire un quadro più ampio per la protezione dei dati nel sistema d'informazione del mercato interno, nonché a garantire la certezza del diritto e un livello più elevato di protezione dei dati.



Viste le prospettive di crescita del sistema d'informazione del mercato interno, sono necessarie una forte base giuridica e ulteriori garanzie per la protezione dei dati.

3.9.2. Body scanner

Nel febbraio 2010 un rappresentante del GEPD ha visionato i body scanner utilizzati in via sperimentale presso l'aeroporto olandese di Schiphol allo scopo di ottenere informazioni aggiuntive sui cosiddetti "sistemi di seconda generazione", che hanno l'obiettivo di migliorare la protezione dei dati e di applicare il principio della tutela della vita privata sin dalla progettazione.

Nel luglio 2010 il GEPD ha pubblicato osservazioni⁽¹⁵⁾ riguardo alla comunicazione sull'impiego dei body scanner negli aeroporti adottata dalla Commissione in giugno⁽¹⁶⁾.

In queste osservazioni, il GEPD ha sottolineato che il **consenso non** può essere usato come giustificazione per legittimare il trattamento dei dati personali ove manchi la base giuridica di tale trattamento.

Ha rilevato anche che, nel caso dei body scanner, l'espressione "**migliori tecniche disponibili**" si riferisce allo stadio più efficace e avanzato dello sviluppo delle attività e dei loro metodi operativi che denotano l'idoneità pratica di determinate tecniche a garantire il rispetto di una particolare soglia di rilevazione in conformità al quadro comunitario sulla protezione della vita privata e dei dati.

Il GEPD continuerà a seguire da vicino gli sviluppi sotto il profilo legislativo e tecnico correlati ai body scanner e darà ogni opportuno contributo alle altre misure che la Commissione europea intende adottare nel 2011.

3.9.3. Sistemi di garanzia dei depositi

I sistemi di garanzia dei depositi rimborsano ai depositanti il valore dei loro depositi fino a un massimo di EUR 100 000 in caso di fallimento di un istituto di credito. La normativa europea relativa a tali sistemi è in vigore dal 1994. Questo strumento è stato potenziato poco tempo dopo che era scoppiata la crisi finanziaria nel 2008, e nel luglio 2010 la Commissione ha avanzato un'altra proposta volta a semplificare e armonizzare le pertinenti norme nazionali.

⁽¹⁵⁾ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-07-01_Security_scanners_EN.pdf

⁽¹⁶⁾ Comunicazione COM(2010) 311 definitivo.



Dai body scanner agli scanner di sicurezza, la soluzione è la tutela della vita privata fin dalla progettazione.

Per il rimborso dei depositi mediante questo sistema di garanzia è necessario il trattamento dei dati dei depositanti. Pertanto trovano applicazione le norme sulla protezione dei dati, qualora i depositanti siano persone fisiche. I dati sono scambiati tra un istituto di credito e un sistema di garanzia dei depositi, ma anche tra gli stessi sistemi di garanzia, o all'interno di uno Stato membro o tra Stati membri diversi.

Il GEPD ha emesso un breve parere su questa proposta nel settembre 2010, nel quale esprime una valutazione complessivamente positiva del modo in cui la proposta ha affrontato gli aspetti correlati alla protezione dei dati. Per esempio, la proposta assicura che i dati personali pertinenti vengono utilizzati soltanto per le finalità per le quali sono stati scambiati, cioè il rimborso dei depositi.

Il GEPD ha poi constatato con particolare soddisfazione che i dati possono essere usati solamente in forma anonima per eseguire i cosiddetti "stress test".

Durante la stesura della proposta, il GEPD aveva infatti messo in dubbio la necessità di utilizzare dati personali per l'esecuzione di tali test.

3.9.4. Iniziativa dei cittadini

L'iniziativa dei cittadini è una delle innovazioni introdotte dal trattato di Lisbona. Attraverso tale iniziativa, almeno un milione di cittadini di un numero significativo di Stati membri possono chiedere alla Commissione di presentare una proposta legislativa su un tema di loro interesse. La raccolta di almeno un milione di dichiarazioni di sostegno comporta il trattamento di dati personali.

Nel parere dell'aprile 2010 il GEPD ha sottolineato che il pieno rispetto delle norme sulla protezione dei dati avrebbe contribuito in misura considerevole all'affidabilità, alla rilevanza e al successo di questo strumento nuovo e importante.

Una delle raccomandazioni riguardava l'obbligo degli organizzatori di un'iniziativa che intendano avvalersi di un sistema di raccolta online di chiedere alle autorità competenti una certificazione della sicurezza del sistema da utilizzare per la raccolta. Per quanto riguarda la tempistica della richiesta, il GEPD ha suggerito di obbligare gli organizzatori a presentare avanzare tale richiesta prima dell'inizio della raccolta delle dichiarazioni di sostegno, piuttosto che dopo. Il GEPD ha suggerito altresì che il legislatore debba garantire:

- che i dati personali raccolti dagli organizzatori non possono essere usati per altre finalità, diverse da quella indicata (cioè di sostenere una data iniziativa dei cittadini);
- che i dati ricevuti dall'autorità competente possono essere usati soltanto allo scopo di verificare l'autenticità delle dichiarazioni di sostegno per una data iniziativa dei cittadini.

3.9.5. Indagine e prevenzione di incidenti e inconvenienti nell'aviazione civile

Nel suo parere il GEPD ha affrontato gli aspetti della proposta che hanno effetti sulla protezione dei dati personali, compreso il **trattamento dei dati contenuti in elenchi di passeggeri e dei dati di vittime, familiari e testimoni**, nelle diverse fasi dell'indagine

e nel contesto dello scambio di informazioni tra le autorità incaricate delle indagini.

Il GEPD ha apprezzato che la proposta tenesse conto degli aspetti relativi alla protezione dei dati; tuttavia, considerato il **contesto specifico** del trattamento dei dati – l'esecuzione di indagini su incidenti nell'ottica di migliorare la sicurezza aerea -, ha ritenuto **necessario fornire ulteriori garanzie per tutelare la riservatezza degli stessi**. In particolare, il GEPD ha suggerito l'introduzione di disposizioni volte a cancellare o rendere anonimi i dati personali quanto prima dal momento in cui gli stessi non sono più necessari per le indagini.

A giudizio del GEPD, occorre adottare garanzie più severe per proteggere le persone direttamente o indirettamente colpite da un incidente grave o dalla perdita di congiunti.

Il GEPD ha raccomandato tra l'altro:

- di tenere riservati, in linea di principio, gli elenchi dei passeggeri, lasciando nel contempo agli Stati membri la possibilità di decidere in casi specifici e per motivi validi, compreso il consenso dei parenti;
- di stabilire periodi limitati per la conservazione dei dati personali;
- di condizionare la trasmissione di dati personali a paesi terzi all'esistenza in questi ultimi di un adeguato livello di protezione;
- di precisare il ruolo e le responsabilità della Commissione europea e dell'Agenzia europea per la sicurezza aerea nel quadro dell'applicazione della normativa sulla protezione dei dati.

3.10. Uno sguardo al futuro

3.10.1. Il progresso tecnologico

In relazioni annuali precedenti ⁽¹⁷⁾ il GEPD aveva già sottolineato la **crescente convergenza** tra il "mondo reale" e il "mondo digitale/di Internet" o la **società dell'informazione**. Di conseguenza, la distinzione tra il mondo reale e quello digitale tende a scomparire. Nel 2010 questa tendenza si

è accentuata perché la convergenza è stata stimolata dall'introduzione su larga scala di strumenti nuovi e innovativi. Finora le persone hanno potuto vivere in realtà parallele scindendo il loro sé virtuale dal loro sé reale, ma tutto ciò sta diventando sempre più difficile e, che lo si voglia o no, stiamo per entrare in un ambiente unico e ininterrotto, che comprende il mondo elettronico al pari di quello reale, ma in cui questi due mondi sono tuttora soggetti a quadri normativi differenti.

Tale tendenza si è materializzata in particolare nelle **reti sociali**, che continuano a espandersi. Oggi-giorno nel mondo si trascorrono oltre 110 miliardi di minuti all'anno usando le reti sociali ⁽¹⁸⁾, e per la prima volta il sito di una rete sociale è diventato il sito più visitato negli Stati Uniti ⁽¹⁹⁾, superando i motori di ricerca.

Il fenomeno è stato viepiù alimentato dai seguenti sviluppi:

- **dispositivi mobili intelligenti** ⁽²⁰⁾: costituiscono uno dei principali pilastri su cui poggiano i ponti che collegano il mondo reale e quello digitale. Sono sempre accesi, sono presenti ovunque e possono condividere, modificare e trattare informazioni in tempo reale. Hanno una capacità di trattamento di dati che è impressionante e attingono alle quasi illimitate risorse disponibili "nella nuvola". Sono in grado di registrare immagini e video in alta definizione, di identificare singolarmente oggetti e persone e di collegare coordinate geografiche a materiale multimediale contenente luoghi, eventi e persone. Gli utenti sono costantemente collegati alla rete per trattare dati personali o per far trattare i loro dati personali;
- **tecniche di riconoscimento facciale**: finora rimaste circoscritte ad ambienti ben controllati, ricevono adesso un nuovo impulso perché cominciano a essere utilizzate nelle reti sociali e nei telefoni intelligenti. La massa di milioni di utenti delle reti sociali che, grazie a dispositivi mobili intelligenti, caricano fotografie che consentono il riconoscimento facciale delle persone ritratte amplia in misura drammatica l'ambito di applicazione di queste tecniche e contribuisce persino al loro miglioramento. Questa nuova tendenza emergente potrebbe anche portare

⁽¹⁸⁾ <http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/#>

⁽¹⁹⁾ <http://www.hitwise.com/us/press-center/press-releases/facebook-was-the-top-search-term-in-2010-for-sec/>

⁽²⁰⁾ <http://www.enisa.europa.eu/media/news-pictures/smartphones-video-clip>

⁽¹⁷⁾ Relazione annuale 2007, pag. 56, e relazione annuale 2009, pag. 64.

alla creazione, a partire dalle piattaforme delle reti sociali, di banche di dati biometrici di dimensioni mai viste prima.

Il concetto di **realtà aumentata** supportata da piattaforme quali i telefoni intelligenti permetterà l'inserimento online di informazioni aggiuntive nella realtà delle singole persone. Già ora è possibile visitare una città e ottenere informazioni aggiuntive sui monumenti che vengono "individuati" da un dispositivo mobile intelligente. Assieme alle tecniche di riconoscimento facciale e alle reti sociali, come descritto prima, nel prossimo futuro diventerà tecnicamente possibile fotografare qualcuno per strada e accedere in tempo reale a informazioni dettagliate su quella persona.

In futuro, anche la **tecnologia indossabile** fungerà da ponte e promuoverà la fusione tra la vita quotidiana reale di una persona e contesti digitali che non necessariamente saranno soggetti al medesimo quadro normativo. Questa tecnologia collegherà i dati sensibili delle persone (temperatura, pressione sanguigna, battito cardiaco, glicemia, eccetera) ad applicazioni e servizi online.

Questi mondi interconnessi e senza soluzione di continuità offrono vantaggi inediti ai cittadini, alle imprese e ai governi, ma comportano anche **minacce senza precedenti** che dovranno essere affrontate in maniera appropriata. In particolare, tra non molto il **furto di identità nel mondo virtuale** avrà conseguenze simili a quelle del furto di identità nel mondo reale. Alla luce di questo fatto, la disponibilità in una rete di quantità massicce di dati personali, la mancata attenzione alle violazioni di dati personali (molte delle quali avvengono a nostra insaputa) e la crescente disponibilità di servizi commerciali, governativi e sociali ai quali è possibile accedere grazie alle identificazioni virtuali nel mondo online costituiscono una miscela potenzialmente pericolosa. Le identità tradizionali, fondate su supporti cartacei, non rappresentano più una soddisfacente soluzione di supporto o di ripiego in caso di compromissione dell'identità elettronica, perché i due tipi di identità diventano sempre più compenetrati l'uno nell'altro.

Quindi, per quanto i confini tra mondo reale e mondo virtuale stiano diventando sempre più indefiniti, le norme vigenti nei due mondi non sono simili, come dimostra il caso dei contatori intelligenti: la produzione, commercializzazione e l'utilizzo dei contatori intelligenti sono disciplinati da una serie di norme specifiche volte a tutelare i consumatori; ma, non appena un contatore è connesso alla rete e comincia a descrivere il comportamento di una persona – diventando, così, un contatore

intelligente – attraverso, per esempio, la registrazione e la conservazione dei dati su quando una persona consuma elettricità, rivelando in tal modo se la persona è a casa oppure no quelle norme possono risultare non più applicabili. La **revisione del quadro di protezione dei dati** potrebbe fornire l'occasione giusta per affrontare tali questioni. Un quadro giuridico deve contribuire all'attuazione delle necessarie garanzie che i cittadini si aspettano di trovare in questo nuovo ambiente di cui si devono poter fidare.

3.10.2. Priorità per il 2011

Nel dicembre 2010 il GEPD ha pubblicato il suo quinto inventario pubblico in qualità di consulente su proposte riguardanti la legislazione comunitaria e ha indicato le proprie priorità nel campo della consultazione per il 2011. Come già negli anni precedenti, il GEPD intende esprimere il proprio parere su tutte le proposte legislative che hanno un impatto sostanziale sulla protezione dei dati, senza peraltro trascurare le misure non legislative qualora esse sollevino questioni non trascurabili di protezioni dei dati.

Le principali priorità del GEPD, delineate nell'inventario, sono indicate in appresso.

- **Revisione del quadro giuridico della protezione dei dati**, che sarà una delle priorità fondamentali del GEPD nel 2011.

- **Varie iniziative riguardanti l'ulteriore attuazione del programma di Stoccolma nello spazio di libertà, sicurezza e giustizia**, quali l'elaborazione di un sistema a entrata-uscita e del programma per viaggiatori registrati, la proposta di direttiva sull'utilizzo dei dati del codice di prenotazione a fini di applicazione della legge e l'introduzione di un TFTP europeo. Inoltre, il GEPD seguirà da vicino le trattative per la conclusione di accordi sulla protezione dei dati con paesi terzi. Infine, ma non meno importante, il GEPD parteciperà attivamente alla revisione della direttiva sulla conservazione dei dati.

- **Attenta valutazione di iniziative nel settore della tecnologia** che potrebbero avere conseguenze sulla protezione della vita privata e dei dati. Il GEPD continuerà a seguire la successiva attuazione dell'**agenda digitale** per l'Europa.

- **Ogni altra iniziativa** che possa comportare effetti significativi per la protezione dei dati, come le iniziative nel settore dei **trasporti** (ad es., l'utilizzo di body scanner negli aeroporti, pacchetti per la mobilità elettronica) e gli scambi di dati su larga scala che possono avvenire nel **sistema d'informazione del mercato interno**.

4

COOPERAZIONE

4.1. Gruppo di lavoro Articolo 29

Il gruppo di lavoro Articolo 29 è un organo consultivo indipendente istituito ai sensi dell'articolo 29 della direttiva sulla protezione dei dati (95/46/CE) e fornisce alla Commissione europea consulenza indipendente su questioni inerenti alla protezione dei dati, oltre a contribuire alla definizione di politiche armonizzate per la protezione dei dati negli Stati membri dell'Unione europea ⁽²¹⁾.

I suoi compiti sono stabiliti nell'articolo 30 della direttiva e si possono sintetizzare come segue:

- fornire alla Commissione europea consulenza di esperti a livello nazionale su questioni attinenti alla protezione dei dati;
- promuovere un'applicazione uniforme dei principi generali della direttiva in tutti gli Stati membri attraverso la cooperazione tra le autorità di controllo della protezione dei dati;
- fornire alla Commissione consulenza in merito a qualsiasi misura che incida sui diritti e sulle

libertà delle persone fisiche in relazione al trattamento di dati personali;

- formulare raccomandazioni destinate alla pubblica opinione, in generale, e alle istituzioni comunitarie, in particolare, su questioni correlate alla protezione delle persone in relazione al trattamento di dati personali nell'Unione europea.

Il GEPD è membro del gruppo di lavoro Articolo 29 dall'inizio del 2004 e lo considera una piattaforma molto importante per la cooperazione con le autorità nazionali di controllo. È evidente altresì che il gruppo di lavoro deve svolgere un ruolo centrale nell'applicazione uniforme della direttiva e nell'interpretazione dei suoi principi generali.

Nel 2010 il gruppo di lavoro ha focalizzato le proprie attività sui quattro temi strategici principali, individuati nel suo programma di lavoro per il 2010-2011, ossia:

- attuare la direttiva e predisporre un quadro giuridico generale per il futuro;
- affrontare la questione della globalizzazione;
- rispondere alle sfide tecnologiche;
- rendere più efficace l'operato del gruppo di lavoro e delle autorità di protezione dei dati.

⁽²¹⁾ Il gruppo di lavoro è formato da rappresentanti delle autorità nazionali di controllo di ciascuno Stato membro, da un rappresentante dell'autorità creata per le istituzioni e gli organismi comunitari (cioè il GEPD) e da un rappresentante della Commissione. Al segretariato del gruppo provvede la Commissione. Sono inoltre presenti come osservatori le autorità nazionali di controllo di Islanda, Norvegia e Liechtenstein (in qualità di partner SEE).

A tal fine il gruppo di lavoro ha adottato vari documenti, tra i quali:

- il parere 2/2010 sulla **pubblicità comportamentale online** (WP 171);
- il parere 5/2010 sulla proposta dell'industria relativa a un quadro per la realizzazione di valutazioni dell'impatto delle **applicazioni RFID** sulla protezione della vita privata e dei dati (WP 175);
- il parere 7/2010 concernente la comunicazione della Commissione europea relativa all'**approccio globale al trasferimento dei dati del codice di prenotazione** (PNR) a paesi terzi (WP 178).

Il gruppo di lavoro e il GEPD hanno collaborato strettamente su questioni riguardanti l'applicazione della direttiva 95/46/CE e l'interpretazione di alcune delle sue disposizioni chiave. Il GEPD ha contribuito attivamente in varie aree, quali:

- il parere 1/2010 sui **concetti di "responsabile del trattamento" e "incaricato del trattamento"** (WP 169);
- il parere 3/2010 sul **principio di responsabilità** (WP 173);
- il parere 8/2010 sul **diritto applicabile** (WP 179).

Il GEPD collabora anche con le autorità nazionali di controllo laddove ciò è necessario per l'espletamento delle proprie funzioni, in particolare scambiando tutte le informazioni utili e chiedendo o prestando assistenza nell'esecuzione dei loro compiti (articolo 46, lettere f) e i) del regolamento). A tale cooperazione di procede caso per caso.

La collaborazione diretta con le autorità nazionali è un fattore sempre più importante nel contesto dello sviluppo di grandi sistemi internazionali come Eurodac, che necessitano di un approccio coordinato alla vigilanza (cfr. sezioni 4.2 e 4.3).

4.2. Controllo coordinato di Eurodac

Un controllo efficace di Eurodac si fonda su una stretta cooperazione tra le autorità nazionali di protezione dei dati e il GEPD.

Le attività del gruppo di coordinamento del controllo di Eurodac, formato da rappresentanti delle autorità nazionali di protezione dei dati e del GEPD, si sono ispirate al programma di lavoro 2010-2011 adottato all'inizio del 2010.

Questo programma di lavoro, pur comprendendo temi diversi, riserva un'attenzione particolare alle questioni comuni o sensibili sulle quali il gruppo di coordinamento può rappresentare un valore aggiunto e fare la differenza. Tuttavia, numerose attività dipendono dall'adozione dei nuovi regolamenti Eurodac e di Dublino, che saranno applicati nel momento opportuno.

Adesso le attività del gruppo sono organizzate in base a uno scadenario, per una migliore pianificazione degli impegni futuri. Il lavoro previsto per i prossimi anni è diviso tra attività da svolgere:

- ogni quattro anni: ad esempio, un audit completo della sicurezza ad opera delle autorità di protezione dei dati a livello sia nazionale sia comunitario. Una preparazione coordinata di questo audit da parte del gruppo di lavoro permetterà di aumentare l'efficienza e di ottenere risultati più comparabili;
- ogni due anni: ad esempio, ispezioni coordinate. Ciò comporta la definizione e l'esecuzione di ispezioni coordinate periodiche;
- ogni anno: attività di investigazione più brevi e con un raggio d'azione più limitato rispetto alle ispezioni coordinate. Saranno eseguite in base alle esigenze individuate dal gruppo;
- su base permanente: per lo più attività di follow-up necessarie a livello strutturale, a titolo di follow-up di sviluppi legislativi e politici, di ricerche speciali e di raccomandazioni precedenti.

All'interno di queste categorie, nel 2010 sono stati selezionati e avviati diversi tipi di attività.

Nel corso del 2010 il gruppo si è riunito a Bruxelles tre volte (in marzo, ottobre e dicembre). Nella riunione di marzo ha rieletto presidente il Garante europeo della protezione dei dati Peter Hustinx e ha eletto vicepresidente Elisabeth Wallin, dell'autorità svedese di protezione dei dati.

Il gruppo ha cominciato a lavorare alla **preparazione dell'audit completo di sicurezza**. È stato nominato un sottogruppo che ha anzitutto individuato i punti nodali della propria attività, come la compilazione di un elenco di obiettivi della sicurezza, e si è poi occupato delle sfide correlate all'esigenza di conseguire risultati comparabili. Il lavoro del sottogruppo proseguirà nel 2011.

Alla fine del 2010 è stata lanciata una **nuova ispezione coordinata**. Il gruppo ha scelto il tema della cancellazione preventiva di dati; a tale proposito, ha esaminato un questionario e affrontato questioni

metodologiche. I risultati sono attesi nel corso del 2011. La cancellazione anticipata di dati è stata considerata una tematica importante in considerazione sia del suo impatto sulla qualità dei dati in Eurodac, sia della protezione delle persone che non dovrebbero più essere registrate nella banca dati.

L'**interazione con le parti interessate** ha avuto un avvio molto positivo durante la riunione di dicembre, cui hanno partecipato anche rappresentanti dell'Alto Commissariato delle Nazioni Unite per i rifugiati e del Consiglio europeo per i profughi e gli esiliati. Le parti interessate esterne hanno illustrato il loro lavoro e le loro priorità e hanno avuto uno scambio di opinioni con il gruppo di lavoro su questioni quali il futuro del sistema di Dublino, le informazioni da dare ai richiedenti asilo e la tutela dei loro diritti. Le parti interessate hanno inoltre motivato la loro contrarietà alla possibilità di consentire alle autorità responsabili dell'applicazione della legge di accedere a Eurodac. Questo scambio di opinioni si è rivelato estremamente utile e dovrebbe essere ripetuto a intervalli regolari.



Il controllo coordinato di Eurodac è essenziale per garantire i diritti delle persone vulnerabili, come i richiedenti asilo.

4.3. Controllo del sistema d'informazione doganale (SID)

La finalità del sistema d'informazione doganale (SID) è di creare un **sistema di allarme** all'interno del quadro della **lotta antifrode** al fine di permettere a qualsiasi Stato membro di accedere ai dati contenuti nel sistema per chiedere a un altro Stato membro di eseguire rilevamenti e rendiconti, sorveglianza discreta, controlli specifici oppure analisi operative e strategiche.

Il SID memorizza informazioni su merci, mezzi di trasporto, persone e società nonché sui beni e i contanti trattenuti, sequestrati o confiscati, al fine di contribuire a prevenire, investigare e perseguire azioni che costituiscono violazioni delle norme doganali e agricole (l'ex "primo pilastro" dell'Unione europea) o gravi contravvenzioni di norme nazionali (l'ex "terzo pilastro" dell'UE). Quest'ultima parte è sottoposta alla vigilanza di un'autorità comune di controllo formata da rappresentanti delle autorità nazionali di protezione dei dati.

Il gruppo di coordinamento del controllo del SID è strutturato come una piattaforma nella quale le autorità di protezione dei dati che sono responsabili del controllo del SID in virtù del regolamento (CE) n. 766/2008 ⁽²²⁾ – cioè il GEPD e le autorità nazionali di protezione dei dati – collaborano conformemente alle rispettive responsabilità, al fine di garantire un controllo coordinato del SID.

Il gruppo di coordinamento:

- a) esaminerà i problemi di attuazione in relazione alle operazioni del SID;
- b) esaminerà le difficoltà incontrate durante i controlli eseguiti dalle autorità di controllo;
- c) esaminerà le difficoltà di interpretazione e applicazione del regolamento SID;

⁽²²⁾ Regolamento (CE) n. 766/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, recante modifica del regolamento (CE) n. 515/97 del Consiglio, relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola.

- d) redigerà raccomandazioni per soluzioni comuni a problemi esistenti e
- e) si impegnerà a migliorare la cooperazione fra le autorità di controllo.

Nel 2010 il GEPD ha convocato due riunioni del gruppo di coordinamento del controllo del SID (in marzo e dicembre). Alle riunioni hanno partecipato rappresentanti delle autorità nazionali di protezione dei dati, dell'autorità comune di controllo in materia doganale e del segretariato della protezione dei dati.

Nella riunione di dicembre il gruppo ha adottato un regolamento interno che disciplinerà la sua attività futura con il SID e ha discusso possibili azioni da compiere nel 2011-2012 per garantire un controllo generale della protezione dei dati del sistema.

4.4. Cooperazione di polizia e giudiziaria: cooperazione con OCC/ACC e GLPG

Il GEPD ha collaborato anche con le autorità responsabili del controllo di determinati organismi o sistemi informatici europei su larga scala, come gli organi comuni di controllo (OCC) di Europol ed Eurojust e le autorità di controllo comuni (ACC) del sistema d'informazione Schengen (SIS), nonché degli aspetti relativi all'ex "terzo pilastro" del sistema d'informazione doganale (SID). Questa cooperazione avviene in forma d'informazione reciproca su temi di interesse comune, ad esempio sui sistemi dei quali il GEPD e gli OCC/ACC controllano ciascuno una parte.

Nel 2010 la cooperazione si è incentrata sul sistema d'informazione doganale. Poiché il GEPD e l'autorità comune di controllo di questo sistema condividono le funzioni di controllo del sistema, è opportuno che coordinino quanto più possibile le rispettive azioni. In tale spirito, il GEPD ha invitato rappresentanti dell'ACC alle riunioni in cui si è discusso del controllo coordinato del SID (cfr. sezione 4.3).

Il GEPD ha inoltre partecipato alle riunioni e alle attività del gruppo di lavoro Polizia e giustizia (GLPG). Nel 2010 il gruppo si è occupato di diverse questioni, tra cui l'elaborazione di una politica comune di controllo e gli accordi "simili a Prüm" (accordi bilaterali sullo scambio di dati). Il GLPG ha anche collaborato con il gruppo di lavoro

Articolo 29 (GLA29) per fornire all'accordo UE-USA sulla protezione dei dati un "contributo comune delle autorità comunitarie di protezione dei dati" rappresentate in questi gruppi di lavoro. In tale circostanza è emersa l'esigenza di un'ampia collaborazione tra i due gruppi in un contesto nel quale la distinzione tra l'ex primo e l'ex terzo pilastro sta perdendo sempre più di significato.

Infine, il gruppo di lavoro Polizia e giustizia si è occupato del proprio futuro, alla luce dei cambiamenti su citati e nella prospettiva di un crescente coinvolgimento del gruppo di lavoro Articolo 29 in aree tradizionalmente di competenza del GLPG.

4.5. Conferenza europea

Le autorità di protezione dei dati degli Stati membri dell'Unione europea e il Consiglio d'Europa si riuniscono annualmente in occasione di una conferenza di primavera per discutere questioni di interesse comune e scambiarsi informazioni ed esperienze su vari argomenti.

La Conferenza europea delle autorità di protezione dei dati si è svolta a **Praga il 29-30 aprile 2010**, aveva come titolo "Analizzare il passato, pensare al futuro" ed è stata ospitata dall'autorità ceca di protezione dei dati.

Nell'ambito della conferenza sono state organizzate sessioni dedicate a vari temi, tra cui: 1) L'Internet delle cose; il controllo onnipresente nel tempo e nello spazio (con una presentazione del Garante aggiunto). 2) Minori in trappola nelle reti. 3) La protezione dei dati personali a un bivio (con una presentazione del GEPD). 4) Il settore pubblico: partner rispettato o incaricato privilegiato del trattamento?

Non sorprende che il **quadro futuro della protezione dei dati** che la Commissione europea sta preparando sia stato un tema centrale delle discussioni. Sono state adottate numerose risoluzioni, in particolare sui temi seguenti:

- il previsto accordo UE-USA sugli standard della protezione dei dati nello spazio della cooperazione di polizia e giudiziaria in materia penale;
- body scanner;

- tutela dei minori;
- il futuro della tutela della vita privata.

4.6. Conferenza internazionale

Le autorità di protezione dei dati e i garanti della vita privata provenienti dai paesi europei e da altre parti del mondo, tra cui Canada, America latina, Australia, Nuova Zelanda, Hong Kong, Giappone e altre giurisdizioni della regione Asia-Pacifico, si riuniscono annualmente in autunno nell'ambito di una conferenza.

Quest'anno la Conferenza internazionale delle autorità di protezione dei dati è stata organizzata dall'autorità israeliana a **Gerusalemme il 26-29 novembre 2010**. Il tema principale di cui si è occupata è stato "Tutela della vita privata: generazioni".

Sono state organizzate numerose sessioni plenarie per discutere delle seguenti tematiche:

- Dove siamo adesso? Il cambiamento intergenerazionale nella percezione della tutela della vita privata
- L'agenda normativa: ascoltare i legislatori
- Tutela della vita privata fin dalla progettazione
- Il futuro della tutela della vita privata: come le norme in materia possono orientare la regolamentazione.

La conferenza ha esaminato inoltre le prospettive delle diverse generazioni per quanto attiene alla protezione della vita privata e dei dati. Uno dei temi importanti affrontati nel corso della conferenza è stato il modo in cui le leggi e i meccanismi di autoregolamentazione influenzano la tecnologia, e vice versa, mentre un altro argomento centrale è stato la crescente diffusione delle reti sociali.

Durante la conferenza, il GEPD e il Garante aggiunto hanno tenuto interventi e presieduto diverse sessioni.

La sessione chiusa dei garanti ha adottato varie risoluzioni, la più importante delle quali è stata la richiesta di organizzare una conferenza intergovernativa in vista della definizione di uno strumento

internazionale vincolante per la protezione della vita privata e dei dati.

La 33ª Conferenza internazionale si svolgerà in Messico nel novembre 2011.

4.7. Organizzazioni internazionali (Seminario di Firenze)

Insieme con l'Istituto universitario europeo, il GEPD ha organizzato il 3° seminario sulla protezione dei dati nelle organizzazioni internazionali. Il seminario si è tenuto a Firenze il 27 e 28 maggio 2010 e ha visto la partecipazione di importanti organizzazioni internazionali, come l'Alto Commissariato delle Nazioni Unite per i rifugiati, l'Organizzazione mondiale del commercio, l'Organizzazione internazionale per le migrazioni, il Tribunale penale internazionale e molte altre. Le discussioni hanno riguardato le numerose sfide che le organizzazioni internazionali devono affrontare per garantire un buon livello di protezione dei dati in contesti talora difficili e senza una chiara base giuridica. Queste organizzazioni, che possono già vantare un buon livello di protezione dei dati, hanno messo in evidenza i molti benefici che essa può apportare alle loro attività fondamentali (ad esempio, sicurezza dei dati e legittimità, in particolare).

Dopo il seminario il GEPD ha diffuso un questionario per fare il punto degli accordi sulla protezione dei dati (o sulla loro mancanza) nelle organizzazioni internazionali che avevano partecipato al seminario. Il questionario era incentrato sui modi per garantire una protezione dei dati reale ed efficace, piuttosto che su specifici accordi legislativi.

Il questionario si fonda pertanto sul lavoro già compiuto dai vari forum internazionali per la protezione dei dati riguardo al concetto di responsabilità, inteso come uno strumento per indurre i responsabili del trattamento ad abbassare ulteriormente il rischio di non-conformità attraverso l'adozione di meccanismi pratici, in grado di garantire un'efficace protezione dei dati. Questo concetto è particolarmente appropriato per le organizzazioni internazionali perché può essere applicato a prescindere dal contesto giuridico nel quale i dati sono trattati.

Le risposte al questionario serviranno da base di riferimento per future azioni in questo ambito. Molti partecipanti hanno espresso l'auspicio che in futuro si tengano periodicamente altri seminari di questo tipo.

5

COMUNICAZIONE

5.1. Introduzione

L'informazione e la comunicazione svolgono un ruolo centrale nell'assicurare la **visibilità** delle principali attività del GEPD e nel **sensibilizzare** l'opinione pubblica sia sull'operato del GEPD sia sulla protezione dei dati in generale. Si tratta di una questione particolarmente importante perché è necessario consolidare ulteriormente la consapevolezza del ruolo e della missione, nonostante i considerevoli progressi già compiuti in tal senso. Indicatori quali il numero delle richieste di informazioni inviate dai cittadini, le indagini dei media e le richieste di interviste, il numero dei sottoscrittori della newsletter, come pure gli inviti a tenere discorsi in occasione di conferenze e il numero di accessi al sito Internet confermano che il GEPD è diventato un punto di riferimento per le questioni connesse con la protezione dei dati a livello comunitario.

L'accresciuta visibilità del GEPD in ambito istituzionale assume un rilievo particolare per i suoi tre ruoli principali: il ruolo di controllo nei confronti di tutte le istituzioni e gli organismi dell'Unione europea coinvolti nel trattamento di dati personali, il ruolo di consulenza per le istituzioni (Commissione, Consiglio e Parlamento) che partecipano all'elaborazione e adozione di norme e politiche nuove che possono avere un impatto sulla protezione dei dati personali e il ruolo di cooperazione con le autorità nazionali di controllo e i vari organi di controllo nel campo della sicurezza e della giustizia.

Anche nel 2010 le attività del GEPD hanno avuto come obiettivo l'ulteriore miglioramento delle azioni di comunicazione e degli strumenti d'informazione

del Garante. Un significativo passo avanti in tal senso è stata l'introduzione del tedesco come terza lingua, accanto all'inglese e al francese, nelle attività di comunicazione e nei rapporti con la stampa – un fatto tanto più rilevante ove si consideri che il tedesco è la madrelingua più diffusa nell'Unione europea. Lo scopo ultimo è quindi quello di raggiungere un pubblico più ampio e dare ai media e ai cittadini di lingua tedesca la possibilità di seguire le attività del GEPD nella loro lingua.

5.2. "Caratteristiche" della comunicazione

La politica di comunicazione del GEPD deve essere costruita secondo caratteristiche specifiche che sono rilevanti in considerazione dell'età, delle dimensioni e delle funzioni dell'istituzione. È quindi necessario un approccio su misura che si avvalga degli strumenti più appropriati per mirare al pubblico giusto, pur rimanendo adattabile a una serie di vincoli e requisiti.

5.2.1. Pubblico e gruppi di riferimento

Diversamente dalla maggior parte delle altre istituzioni comunitarie, le cui politiche e attività in materia di comunicazione si collocano su un piano generale e si rivolgono ai cittadini dell'UE nel loro insieme, la sfera d'azione diretta del GEPD è molto più distinta e si focalizza principalmente sulle istituzioni e gli organismi comunitari, sugli interessati, in generale, e sui dipendenti dell'Unione europea, in particolare,

nonché sui soggetti politici comunitari e sui “collegli della protezione dei dati”. Ne consegue che la politica di comunicazione del GEPD non ha bisogno di passare attraverso una strategia di “comunicazione di massa”; anzi, la sensibilizzazione dei cittadini comunitari sulle questioni legate alla protezione dei dati negli Stati membri dipende essenzialmente da un approccio più indiretto, ad esempio per il tramite delle autorità di protezione dei dati a livello nazionale.

In ogni caso, il GEPD si adopera per aumentare la propria visibilità verso il pubblico, specialmente attraverso una serie di strumenti di comunicazione (sito Internet, newsletter, eventi di sensibilizzazione), contatti periodici con le parti interessate (visite di studio presso i propri uffici, ad esempio) e la partecipazione a eventi pubblici, incontri e conferenze.

5.2.2. Politica linguistica

La politica di comunicazione del GEPD deve anche tener presente il carattere specifico del suo settore di attività. Le questioni relative alla protezione dei dati possono essere considerate alquanto tecniche e oscure per i non esperti, e quindi il linguaggio che il GEPD utilizza per comunicare dovrebbe essere adattato di conseguenza. Quando si tratta di strumenti d’informazione e comunicazione destinati a ogni tipo di pubblico, occorre utilizzare uno stile chiaro e comprensibile, evitando tecnicismi inutili. Si stanno perciò compiendo continui sforzi in tal senso, soprattutto per comunicare con un pubblico vasto e con i media non specializzati, allo scopo di correggere un’immagine eccessivamente “giuridica” della protezione dei dati.

Nei confronti di un pubblico più informato (ad esempio, specialisti della protezione dei dati, soggetti interessati dell’Unione europea) è invece opportuno ricorrere a un linguaggio più tecnico e specializzato. Pertanto, può essere necessario usare stili di comunicazione e linguaggi differenti per comunicare le stesse informazioni.

5.3. Rapporti con i media

Il GEPD intende essere quanto più accessibile possibile ai giornalisti per mettere l’opinione pubblica in condizione di seguire le sue attività. Tiene i media regolarmente informati mediante comunicati stampa, interviste, dibattiti e conferenze stampa. La gestione delle richieste provenienti dai media offre l’occasione di ulteriori contatti regolari.

5.3.1. Comunicati stampa

Nel 2010 il servizio stampa ha pubblicato 19 comunicati, riguardanti, per la maggior parte, l’attività del GEPD nel settore della consulenza e, più specificamente, i **pareri su nuovi atti legislativi** di rilevanza diretta per i cittadini. Tra le questioni trattate figurano la strategia di riforma della protezione dei dati nell’Unione europea, i negoziati sull’accordo commerciale anticontraffazione (ACTA), l’accordo UE-USA sul programma di controllo delle transazioni finanziarie dei terroristi (TFTP), la gestione delle informazioni nello spazio di libertà, sicurezza e giustizia, la tutela della vita privata e la fiducia nella società dell’informazione, la strategia esterna dell’Unione europea riguardo ai dati contenuti nel codice di prenotazione (PNR), il processo di valutazione della direttiva sulla conservazione dei dati e la strategia comunitaria sulla sicurezza interna. Oggetto di comunicati stampa sono state anche alcune sentenze della Corte di giustizia europea riguardanti la protezione dei dati, come quella nella causa Bavarian Lager e quella sull’indipendenza delle autorità di protezione dei dati.

Inoltre, sono stati diffusi comunicati stampa sulle **attività fondamentali nel settore del controllo**, con particolare attenzione per l’adozione di orientamenti sulla videosorveglianza e una politica complessiva per il controllo della conformità e l’applicazione delle norme.

I comunicati stampa sono stati pubblicati sul sito del GEPD e nella banca dati interistituzionale dei comunicati stampa della Commissione europea (RAPID) in inglese e francese. Nel 2010 è stata introdotta anche una versione in lingua tedesca, coerentemente con l’adozione del tedesco come terza lingua delle attività di comunicazione del GEPD. I comunicati stampa sono stati distribuiti a una rete costantemente aggiornata di giornalisti e parti interessate. Le informazioni contenute nei comunicati stampa ricevono di solito un’ampia copertura mediatica, sia nella stampa generica che in quella specializzata, e spesso sono pubblicati su siti istituzionali e non, tra cui quelli delle istituzioni e degli organismi comunitari, dei gruppi per le libertà civili, di istituzioni accademiche e società commerciali che si occupano di tecnologie dell’informazione.

5.3.2. Interviste

Nel 2010 il GEPD ha rilasciato una ventina di interviste a giornalisti della carta stampata, di emittenti radiotelevisive e dei media elettronici di tutta Europa, con un numero significativo di richieste

provenienti dalla stampa tedesca, austriaca, olandese e statunitense.

Ne sono scaturiti una serie di articoli sulla stampa internazionale, nazionale e comunitaria, sia generica che specializzata nel campo delle tecnologie informatiche, e interviste radiofoniche e televisive (ad esempio, alla televisione nazionale austriaca e alle radio olandese e austriaca).

Le interviste hanno spaziato su vari temi orizzontali, come la tendenza verso una società della sorveglianza e le sfide attuali e future nel campo della protezione della vita privata e dei dati, senza tuttavia trascurare questioni più specifiche di cui si è parlato molto nel 2010, quali l'accordo TFTP con gli Stati Uniti, la revisione del quadro giuridico comunitario per la protezione dei dati e le preoccupazioni per la tutela della vita privata sui siti delle reti sociali, nelle applicazioni di geolocalizzazione e in relazione all'uso di body scanner negli aeroporti.

5.3.3. Conferenze stampa

Una conferenza stampa è stata organizzata il 15 novembre 2010 a Bruxelles sul tema della revisione delle norme comunitarie in materia di protezione dei dati e tutela della vita privata. Peter Hustinx e Giovanni Buttarelli hanno parlato in

particolare della comunicazione della Commissione, pubblicata all'inizio di novembre 2010, sul rafforzamento delle norme comunitarie in materia di protezione dei dati. La conferenza stampa ha altresì offerto l'occasione per presentare la relazione annuale del GEPD relativa al 2009 e delineare i tratti principali delle attività svolte nel 2009 in riferimento alle funzioni di controllo, consulenza e cooperazione (cfr. sezione 5.7.1).

5.3.4. Richieste dei media

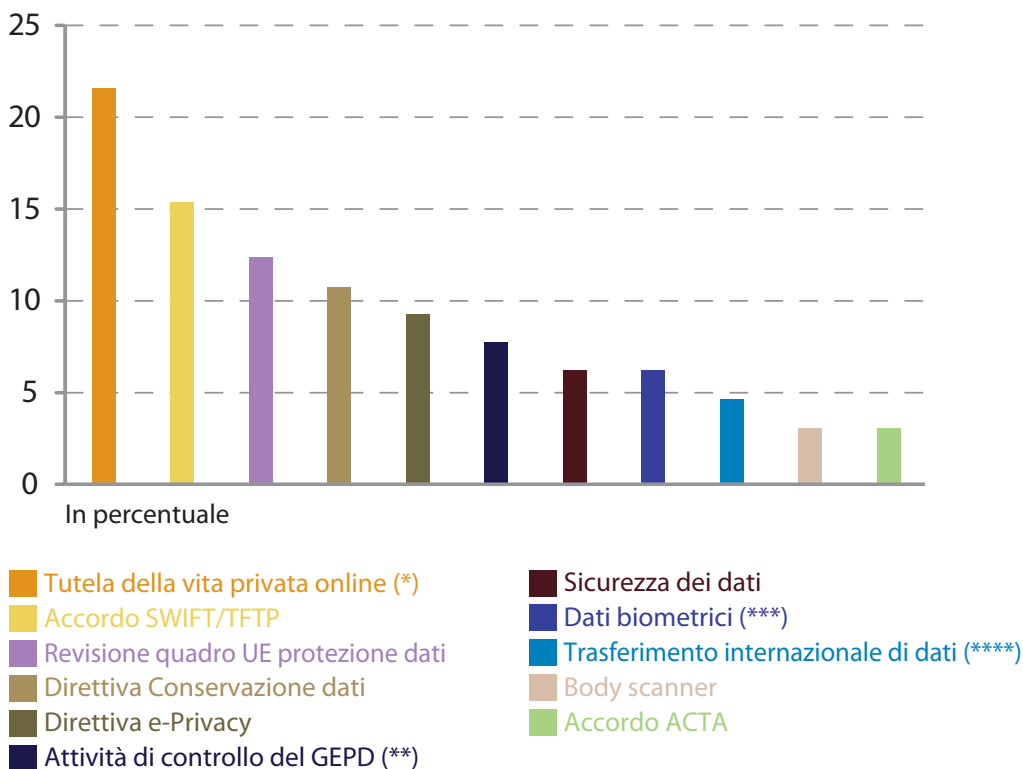
Il GEPD riceve costantemente dai media richieste di vario genere, concernenti tra l'altro osservazioni e chiarimenti o informazioni. Nel 2010 l'attenzione dei media si è incentrata soprattutto sulla questione della tutela della vita privata online, specificamente nelle nuove applicazioni online, come le applicazioni di geolocalizzazione, i motori di ricerca e le reti sociali. La maggior parte delle richieste dei media ha riguardato, appunto, quest'area. Un altro oggetto di particolare interesse tra i media è stato l'accordo con gli Stati Uniti sul trattamento e trasferimento di dati finanziari nel quadro del programma di controllo delle transazioni finanziarie dei terroristi (TFTP).

Gli altri temi che hanno richiamato l'attenzione dei media sono stati la revisione del quadro giuridico comunitario in materia di protezione dei dati, la



La conferenza stampa del GEPD sulla revisione del quadro giuridico comunitario per la protezione dei dati (Bruxelles, 15 novembre 2010)

Principali temi oggetto di richieste da parte della stampa nel 2010



(*) comprese nuove applicazioni online, motori di ricerca e reti sociali

(**) compresi orientamenti su videosorveglianza

(***) compreso sistema d'informazione Schengen

(****) comprese decisioni della Commissione su adeguatezza

direttiva sulla conservazione dei dati, la direttiva sulla e-privacy e le sue disposizioni in merito alla violazione dei dati, le attività di controllo del GEPD, compresi i suoi orientamenti sulla videosorveglianza, il tema della sicurezza dei dati, i dati biometrici – sia nei passaporti che nel sistema d'informazione Schengen – e i trasferimenti internazionali di dati, comprese le decisioni della Commissione sull'adeguatezza dei paesi terzi e l'uso di body scanner negli aeroporti.

5.4. Richieste di informazioni e pareri

Nel 2010 il numero delle richieste di informazioni o assistenza presentate dai cittadini è leggermente diminuito (141 domande rispetto alle 174 del 2009), principalmente a causa di un calo del numero delle richieste concernenti questioni di protezione dei dati a livello nazionale, che esulano dalla competenza del GEPD. Questo andamento può essere interpretato come il risultato degli sforzi volti

a precisare meglio la sfera di competenza del GEPD attraverso i vari strumenti di informazione e comunicazione di cui dispone.

Le richieste di informazioni provengono da una vasta gamma di singoli e parti interessate, che vanno dai soggetti che operano nel contesto comunitario e/o lavorano nel settore della tutela della vita privata, della protezione dei dati e delle tecnologie dell'informazione (studi legali, società di consulenza, lobbisti, ONG, associazioni, università, eccetera) ai cittadini che chiedono maggiori informazioni su questioni riguardanti la tutela della vita privata o aiuto nella risoluzione dei problemi concernenti quest'ultima.

Il primo gruppo di richieste ricevute nel 2010 si riferisce a reclami presentati da cittadini dell'Unione per i quali il GEPD non è competente. Tali reclami riguardano per lo più presunte violazioni della protezione dei dati da parte di pubbliche autorità, società nazionali o private e servizi e tecnologie online, come i giochi d'azzardo online, i blog,

i servizi di geolocalizzazione, le reti sociali e gli strumenti per l'invio di messaggi. Tra gli altri argomenti trattati nelle richieste figuravano la sicurezza dei dati bancari, il diritto di accesso a documenti detenuti da amministrazioni nazionali, la trasmissione a terzi di dati personali senza il consenso della persona interessata, ricorsi contro una decisione di un'autorità nazionale di protezione dei dati. Poiché questi reclami non rientrano nella sfera di competenza del GEPD, questi invia ai presentatori dei reclami una comunicazione in cui si specifica qual è il proprio mandato e li invita a rivolgersi all'autorità nazionale competente, che di norma è l'autorità di protezione dei dati dello Stato membro in questione.

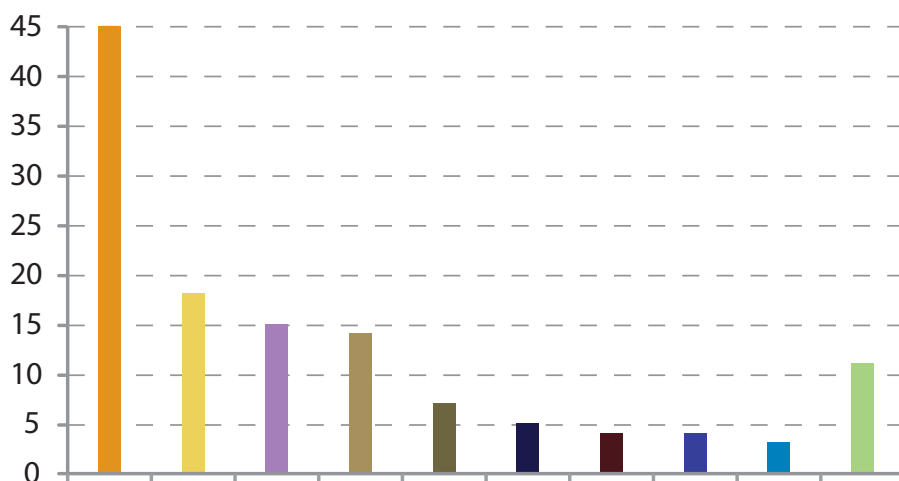
Il secondo gruppo di richieste ricevute nel 2010 si riferisce alla legislazione degli Stati membri dell'Unione europea in materia di protezione dei dati e/o alla sua applicazione a livello nazionale. In questi casi il GEPD consiglia ai richiedenti di contattare la competente autorità di protezione dei dati e, ove del caso, l'unità Protezione dati della Commissione europea.

Le altre richieste d'informazione rientravano per la maggior parte nella sfera di competenza del GEPD e pertanto hanno ricevuto risposte nel merito. Riguardavano, tra l'altro, le attività del GEPD, in particolare nell'ambito della politica e della consulenza, la legislazione comunitaria in materia di protezione dei dati, questioni concernenti la protezione dei dati nell'amministrazione dell'UE, la revisione del quadro comunitario per la protezione dei dati, l'accordo TFTP e i dati bancari, il trasferimento internazionale di dati e l'accesso al sistema d'informazione Schengen.

5.5. Visite di studio

Nel contesto dell'impegno volto ad accrescere ulteriormente la conoscenza della protezione dei dati, nonché ai fini dell'interazione con il mondo accademico, il GEPD riceve regolarmente visite di studenti specializzandi nei campi del diritto europeo, della protezione dei dati e/o della sicurezza informatica. Nel 2010 l'ufficio del Garante ha accolto sette gruppi di studenti di numerosi paesi europei.

Principali temi oggetto di richieste di informazione da parte dei cittadini nel 2010



- Reclami al di fuori della competenza del GEPD
- Normativa nazionale sulla protezione dei dati
- Attività e pareri consultivi del GEPD
- Normativa UE sulla protezione dei dati
- Questioni di protezione dati nell'amministrazione UE
- Revisione del quadro UE sulla protezione dei dati
- Accordo TFTP e dati bancari
- Trasferimento internazionale di dati
- Sistema d'informazione Schengen
- Altro

Nell'ottobre 2010, per esempio, ha ospitato un gruppo di studenti di diritto europeo e internazionale della fondazione tedesca Friedrich-Ebert, ai quali ha illustrato il proprio ruolo e le proprie attività e con i quali ha discusso di questioni inerenti alla protezione dei dati nel quadro del programma di Stoccolma. Altri gruppi di visitatori hanno compreso studenti austriaci partecipanti a un master in amministrazione pubblica e studenti dell'Università olandese di Tilburg, della Fondazione tedesca Rosa Luxemburg e dell'Università francese di Grenoble.

Nell'ottica di raggiungere un pubblico più giovane, l'ufficio del GEPD ha accolto anche un gruppo di studenti austriaci delle scuole superiori con i quali il personale dell'ufficio ha discusso questioni concrete relative alla protezione dei dati che erano particolarmente interessanti per loro, come le reti sociali online.

5.6. Strumenti d'informazione online

5.6.1. Sito Internet

Il sito Internet è il canale di comunicazione e lo strumento informativo più importante del GEPD. Viene aggiornato quasi quotidianamente ed è anche il mezzo attraverso il quale i visitatori possono accedere ai documenti prodotti dal GEPD nell'ambito delle proprie attività (ad esempio, pareri su controlli preventivi e proposte di legislazione comunitaria, priorità di lavoro, pubblicazioni, discorsi del Garante e del Garante aggiunto, comunicati stampa, newsletter, informazioni su eventi).

Sviluppo dei contenuti del sito

Nel 2010 il più importante miglioramento apportato al sito è stata l'introduzione della versione tedesca, in aggiunta a quella inglese e francese. Tale iniziativa è conseguente alla decisione di pubblicare tutto il materiale destinato alla comunicazione esterna in (almeno) queste tre lingue per soddisfare meglio le esigenze d'informazione sia dei cittadini che delle parti interessate.

Inoltre, la pagina iniziale è stata riorganizzata per dare maggiore rilievo alle ultime notizie sulle attività del GEPD.

Sono previsti ulteriori miglioramenti del sito, che comprenderanno:

- l'inserimento di un modulo di reclamo online, per semplificare la procedura di presentazione dei reclami e accelerare la loro gestione da parte dei servizi del GEPD;
- una riorganizzazione della sezione riguardante i pareri su controlli preventivi, per migliorare le capacità di ricerca e la navigabilità tra le diverse categorie tematiche;
- una presentazione semplificata del registro delle notifiche;
- l'introduzione di una sezione dedicata alla stampa, per mettere a disposizione dei professionisti dei media materiale e risorse rilevanti da utilizzare per gli articoli e le interviste.

Traffico e navigazione

Nell'ambito dell'impegno in corso per migliorare le prestazioni del sito, nel 2009 sono state migliorate molte caratteristiche, alcune meno visibili di altre (ad esempio, lo strumento di ricerca avanzata).

Un'analisi dei dati sul traffico e sulla navigazione rivela che nel 2010 il sito ha avuto in totale 108 215 visitatori individuali, con più di 12 000 visite mensili in febbraio e marzo, registrando così un aumento piuttosto significativo rispetto al 2009. Dopo la pagina iniziale, le pagine visitate più spesso sono state quelle dei contatti, del controllo e della consultazione, ma molto popolari sono risultate essere anche le pagine delle notizie, delle pubblicazioni e degli eventi. Dai dati statistici emerge altresì che la maggior parte dei visitatori accede al sito tramite un indirizzo diretto, un segnalibro, un collegamento in un messaggio di posta elettronica o un collegamento da un altro sito – come il portale Europa o il sito di un'autorità nazionale di protezione dei dati. I collegamenti dei motori di ricerca sono utilizzati solo da un numero esiguo di visitatori. Queste cifre ci inducono a ritenere che il sito del GEPD venga consultato da visitatori regolari che si fidano dei suoi contenuti.

5.6.2. Newsletter

La newsletter del GEPD rimane uno strumento prezioso per informare sulle più recenti attività del GEPD e attirare l'attenzione sulle novità apportate al sito. La newsletter fornisce informazioni sui più

recenti pareri del GEPD riguardanti le proposte legislative dell'UE e i controlli preventivi, oltre a contenere ragguagli su conferenze e altri eventi organizzati nel settore e sui discorsi più recenti del Garante e del Garante aggiunto. Le newsletter sono disponibili sul sito del GEPD; è possibile abbonarsi accedendo a questa funzione dalla pagina dedicata.

Nel 2010 sono stati pubblicati cinque numeri della newsletter del GEPD, con una frequenza media di un numero ogni due mesi. Fino al 2010 la newsletter è stata pubblicata in inglese e francese; in quell'anno è stata introdotta anche la versione in lingua tedesca per raggiungere un pubblico più ampio e dar seguito alla decisione di usare tre lingue di lavoro nel servizio stampa del GEPD.

Il numero degli abbonati alla newsletter è salito da 1 200 alla fine del 2009 a circa 1 500 alla fine del 2010. Tra essi figurano deputati al Parlamento europeo, dipendenti delle istituzioni comunitarie e delle autorità nazionali di protezione dei dati, giornalisti, esponenti del mondo accademico, società di telecomunicazione e studi legali.

5.6.3. Intranet

Nell'ottica di migliorare la comunicazione interna e semplificare lo scambio di informazioni tra i diversi settori dell'ufficio del GEPD, è stata istituita un'Intranet, con l'aiuto del competente servizio del Parlamento europeo. Questo nuovo portale interno sarà pienamente operativo all'inizio del 2011.

5.7. Pubblicazioni

5.7.1. Relazione annuale

La relazione annuale è la principale pubblicazione del GEPD. Fornisce un quadro generale delle attività del Garante nei principali settori operativi del controllo, della consultazione e della cooperazione durante l'anno di riferimento, oltre a illustrare i risultati conseguiti in termini di comunicazione esterna e gli sviluppi riguardanti l'amministrazione, il bilancio e il personale.

La relazione può rivestire un interesse particolare per diversi gruppi e individui a livello internazionale, europeo e nazionale – quali, in generale, i soggetti interessati e, in particolare, i dipendenti dell'Unione europea, il sistema delle istituzioni comunitarie, le autorità di protezione dei dati, gli esperti di protezione dei dati, i gruppi d'interesse

e le organizzazioni non governative operanti nel settore, giornalisti e chiunque richieda informazioni sulla protezione dei dati a livello comunitario.

Nel 2010 la relazione è stata migliorata in vari aspetti, sotto il profilo sia formale che sostanziale, per renderla di più facile lettura e mettere chiaramente in evidenza i risultati e le conclusioni più importanti in essa contenuti.

Il 15 novembre 2010 il Garante e il Garante aggiunto hanno presentato la relazione annuale del GEPD per il 2009 alla commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo. Gli elementi principali della relazione sono stati presentati anche alla stampa nella conferenza stampa organizzata lo stesso giorno sul tema del quadro giuridico comunitario in materia di protezione dei dati (cfr. sezione 3.3).



La relazione annuale del GEPD per il 2009

5.7.2. Pubblicazioni tematiche

Sono stati avviati i lavori preparatori per la pubblicazione di "schede" tematiche su questioni strategicamente rilevanti nel settore della protezione dei dati. Lo scopo delle nuove pubblicazioni è di fornire sia al pubblico più vasto sia alle parti interessate informazioni e orientamenti mirati. La prima serie di schede informative tratterà argomenti quali la direttiva sulla e-privacy, l'accordo SWIFT/TFTP e i dati contenuti nel codice di prenotazione (PNR).

5.8. Eventi di sensibilizzazione

Il GEPD è attento a cogliere ogni opportunità che gli consenta di sottolineare la crescente importanza della protezione della vita privata e dei dati, come pure di attirare l'attenzione sui diritti degli interessati e sugli obblighi dell'amministrazione europea riguardo alla protezione della vita privata e dei dati.

5.8.1. Giornata della protezione dei dati

Gli Stati membri e il Consiglio d'Europa, insieme con le istituzioni e gli organismi comunitari, hanno celebrato il 28 gennaio 2010 la quarta Giornata europea della protezione dei dati. In quella data ricorre l'anniversario dell'adozione della Convenzione sulla protezione dei dati personali (Convenzione 108) del Consiglio d'Europa, che è il primo strumento internazionale giuridicamente vincolante nel campo della protezione dei dati.

Negli anni passati, il GEPD ha profitto di tale occasione per ribadire l'importanza della protezione della vita privata e dei dati nonché, in particolare, per sensibilizzare il personale dell'Unione europea sui suoi diritti e doveri in questo settore. Ogni anno viene allestito, in questa circostanza, uno spazio informativo nei locali del Parlamento europeo,

della Commissione europea e del Consiglio, in collaborazione con il responsabile della protezione dei dati di ciascuna istituzione. I visitatori hanno così la possibilità di rivolgere domande ai membri dell'ufficio del GEPD e al responsabile della protezione dei dati e di mettere alla prova le loro conoscenze sulla protezione dei dati nell'UE attraverso un questionario.

Nel 2010 il GEPD ha dato nuovo slancio a questa attività specifica approfondendo ulteriore impegno per sensibilizzare maggiormente il personale dell'Unione europea. Il 28 gennaio 2010 è stata organizzata, presso la Commissione europea, una colazione-dibattito sul tema "Protezione della vita privata e dei dati: in che modo vi riguarda?". Il Garante Peter Hustinx ha tenuto una presentazione per il personale della Commissione e ha risposto alle domande sui diritti connessi con la protezione dei dati e sugli strumenti per esercitarli all'interno dell'amministrazione comunitaria.

Inoltre, un videomessaggio del Garante e del Garante aggiunto ai soggetti istituzionali interessati è stato diffuso e messo a disposizione sul sito per illustrare il ruolo del GEPD e delineare le sfide future.

Il GEPD ha partecipato a numerose manifestazioni svoltesi a Bruxelles in occasione della Giornata della



Peter Hustinx, Garante europeo per la protezione dei dati, mentre interviene alla conferenza "Think Privacy" e alla cerimonia di consegna dei riconoscimenti (Bruxelles, 28 gennaio 2010)

protezione dei dati, come la conferenza e la cerimonia di consegna dei premi che hanno concluso la terza campagna "Think privacy", organizzata dalla European Schoolnet e da Microsoft. Nell'ambito della campagna si è svolto il concorso europeo "Think Privacy", cui hanno partecipato giovani di età compresa tra 15 e 19 anni che hanno creato e proposto una presentazione multimediale dal titolo "La tutela della vita privata è un diritto umano – trattala con cura".

Il 29 e 30 gennaio 2010 il GEPD ha preso parte alla conferenza internazionale "Computer e protezione della vita privata e dei dati", mirata a costruire un ponte tra politici, accademici, professionisti e attivisti per dibattere delle questioni emergenti in materia di protezione della vita privata e dei dati e di tecnologia informatica. Il tema della quarta edizione della conferenza era "Un elemento di scelta", in riferimento alle molte opzioni disponibili per la politica di protezione dei dati. I membri del segretariato del GEPD hanno partecipato a tavole rotonde e il Garante Peter Hustinx ha tenuto il discorso conclusivo della conferenza.

5.8.2. Giornata Porte aperte dell'Unione europea

L'8 maggio 2010 il GEPD ha partecipato, come ogni anno, alla Giornata Porte aperte delle istituzioni europee, organizzata presso il Parlamento europeo a Bruxelles.

La Giornata Porte aperte dell'UE offre un'eccellente occasione per sensibilizzare l'opinione pubblica sulla necessità di proteggere la vita privata e i dati personali.

Il GEPD ha allestito un proprio spazio nell'edificio principale del Parlamento e i dipendenti del segretariato erano presenti per rispondere alle domande dei visitatori. Come nella Giornata della protezione dei dati, presso lo stand del GEPD è stato distribuito materiale informativo ai visitatori, ai quali è stato proposto anche un questionario sulla protezione della vita privata e dei dati a livello comunitario.



Visitatori rispondono a un questionario sulla protezione dei dati durante la Giornata europea della protezione dei dati.

6

AMMINISTRAZIONE, BILANCIO E PERSONALE

6.1. Introduzione

La signora Monique Leens, responsabile amministrativa del segretariato del GEPD sin dalla sua fondazione, è andata in pensione nel giugno 2010. Ha fornito un apporto decisivo alla costruzione dell'ufficio del GEPD negli ultimi sei anni e il GEPD le augura ogni bene per il suo pensionamento, ampiamente meritato. Al suo posto è stato nominato il signor Christopher Docksey, temporaneamente distaccato dai servizi giuridici della Commissione europea, che ha assunto l'incarico di direttore ad interim del GEPD. Il segretariato è stato ulteriormente potenziato con l'arrivo del signor Leonardo Cervera Navas, proveniente anch'egli dalla Commissione europea, in qualità di responsabile del settore Risorse umane, bilancio e amministrazione.

Il numero dei dipendenti è notevolmente aumentato nel corso del 2010. Dopo la pubblicazione della lista di riserva dei concorsi generali per la protezione dei dati organizzati dal GEPD, sono stati assunti dodici nuovi funzionari. Si è reso così necessario non soltanto trovare nuovi uffici per ospitarli, ma anche adottare una nuova struttura organizzativa in grado di soddisfare le esigenze di un'organizzazione più grande, con il compito di gestire responsabilità nuove e complesse.

La riorganizzazione del GEPD, avviata con una nota interna nell'aprile 2010, è proseguita poi durante tutto l'anno con il contributo di un consulente amministrativo esterno. Si prevede che quest'opera di riorganizzazione continui anche nel 2011 e si concentri in particolare sulla gestione della strategia e della prestazione.

6.2. Bilancio

Nel 2010 l'autorità di bilancio ha stanziato per il GEPD un bilancio di EUR 7 104 351, con un aumento del 6,62 % rispetto all'anno precedente.

L'aumento tiene conto delle esigenze di un'organizzazione più grande, con un maggior numero di dipendenti e di attività e con nuove responsabilità conseguenti all'entrata in vigore del trattato di Lisbona. Senza considerare gli stipendi e le spese per gli edifici, una parte consistente del bilancio del GEPD è destinata alle traduzioni, dato che i pareri del GEPD sulle proposte legislative vengono tradotti in tutte le lingue ufficiali dell'Unione europea e pubblicati nella Gazzetta ufficiale dell'Unione europea. I pareri su controlli preventivi e altri documenti pubblicati sono tradotti nelle lingue di lavoro del GEPD (inglese, francese e tedesco).

Nella sua dichiarazione di affidabilità (DDA) relativa al 2009, la Corte dei conti europea non ha chiesto grandi cambiamenti e nella relazione finale ha formulato due sole raccomandazioni: migliorare gli standard di controllo interni adottando un sistema di verifiche ex post e istituire un registro centrale di tutte le eccezioni alle procedure finanziarie standard.

Nel 2010 è proseguita l'assistenza da parte della Commissione europea su questioni finanziarie, specialmente in riferimento ai servizi contabili, perché il Contabile della Commissione è anche il Contabile del GEPD. In tale contesto, la direzione generale Bilancio della Commissione ha eseguito una convalida delle procedure applicate nei sistemi locali di

contabilità, e nella propria relazione al riguardo ha emesso una valutazione positiva. La nomina di un Corrispondente Contabile era la principale raccomandazione contenuta nella relazione.

A tutte le raccomandazioni formulate in queste relazioni dalla Corte dei conti europea e dalla Commissione è stato dato seguito nel modo seguente:

- a) nel flusso finanziario è stato introdotto un nuovo sistema interno di verifica finanziaria;
- b) è stato nominato un Corrispondente Contabile;
- c) è stato istituito un registro centrale delle eccezioni ed
- d) è in corso di adozione un sistema di verifica ex post.

Dopo la riorganizzazione del GEPD, il direttore ad interim Christopher Docksey è stato nominato ordinatore delegato, mentre il responsabile del settore Risorse umane, bilancio e amministrazione Leonardo Cervera Navas è stato nominato viceordinatore delegato. Questa nuova struttura assicura maggiore flessibilità e rafforza il processo di auto-organizzazione delle operazioni finanziarie del GEPD.

Laddove non ci sono norme specifiche, il GEPD applica le norme interne della Commissione per l'esecuzione del bilancio.

6.3. Risorse umane

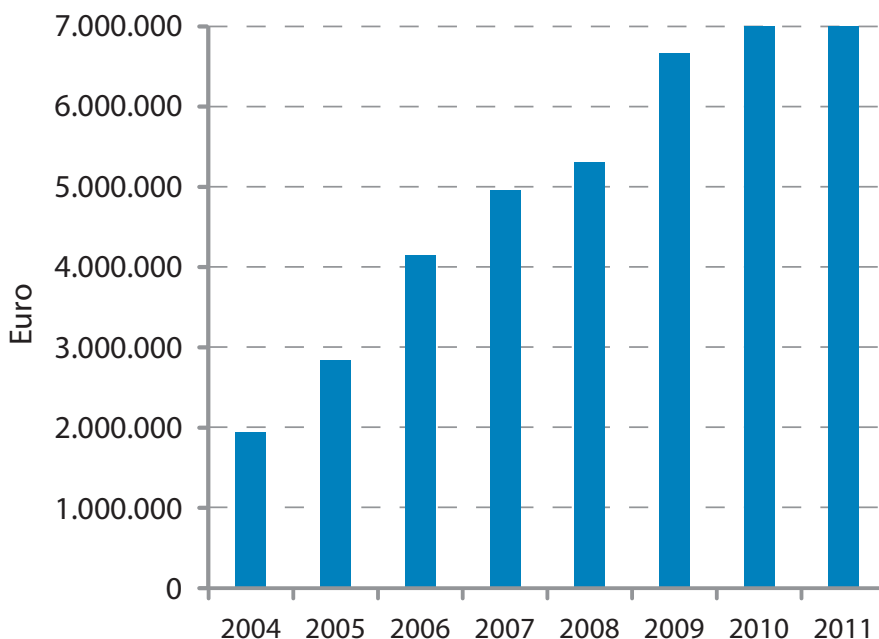
6.3.1. Assunzioni

Come già negli anni passati e come dimostrato in precedenti capitoli della presente relazione, la crescente visibilità del GEPD sta determinando un aumento del carico di lavoro e un'espansione dei compiti da affrontare nella prospettiva delle risorse umane.

Sulla scorta di un accordo sul livello dei servizi, il GEPD ha accesso ai servizi dell'Ufficio europeo di selezione del personale (EPSO) ed è presente nel suo consiglio di amministrazione in qualità di osservatore. In stretta collaborazione con l'EPSO, nel 2009 il GEPD ha bandito un concorso generale sulla protezione dei dati per assumere personale altamente specializzato. Nell'estate del 2010 sono state costituite tre liste di riserva per i gradi AD9, AD6 e AST3. La validità delle liste di riserva è stata estesa quanto meno fino alla fine del 2011.

Dopo la pubblicazione di queste liste, il GEPD ha dato il via a una procedura di assunzione di grandi dimensioni, intervistando i candidati iscritti nelle liste e funzionari di altre istituzioni, conformemente all'articolo 29 dello statuto del personale. Nel 2010 il GEPD ha assunto dodici funzionari e introdotto una nuova categoria di dipendenti: gli agenti a contratto. Tramite una procedura di selezione dei candidati iscritti nelle liste CAST, sono stati assunti

Andamento del bilancio del GEPD 2004-2011



anche due agenti a contratto e, per sopperire a necessità temporanee, nel 2010 è stato reclutato un segretario ad interim. In tutto, nel 2010 il GEPD ha assunto 15 nuovi dipendenti.

Infine, sul sito per il reclutamento interistituzionale è stato pubblicato alla fine del 2010 l'avviso di vacanza del posto di direttore del GEPD. Si ritiene che la procedura di selezione di questo funzionario di alto livello sarà completata entro la prima metà del 2011.

6.3.2. Programma di tirocinio

Nel 2005 è stato istituito un programma di tirocinio allo scopo di offrire ai giovani laureati l'opportunità di mettere in pratica le loro conoscenze accademiche, maturando al contempo un'esperienza pratica nelle attività quotidiane del GEPD. Il programma consente inoltre al GEPD di accrescere la propria visibilità tra i cittadini più giovani dell'Unione europea, specialmente tra gli studenti universitari e i giovani laureati specializzati nel campo della protezione dei dati.

Il programma principale prevede che siano ospitati in media due tirocinanti per ogni sessione, con due sessioni annuali di cinque mesi ciascuna (da marzo

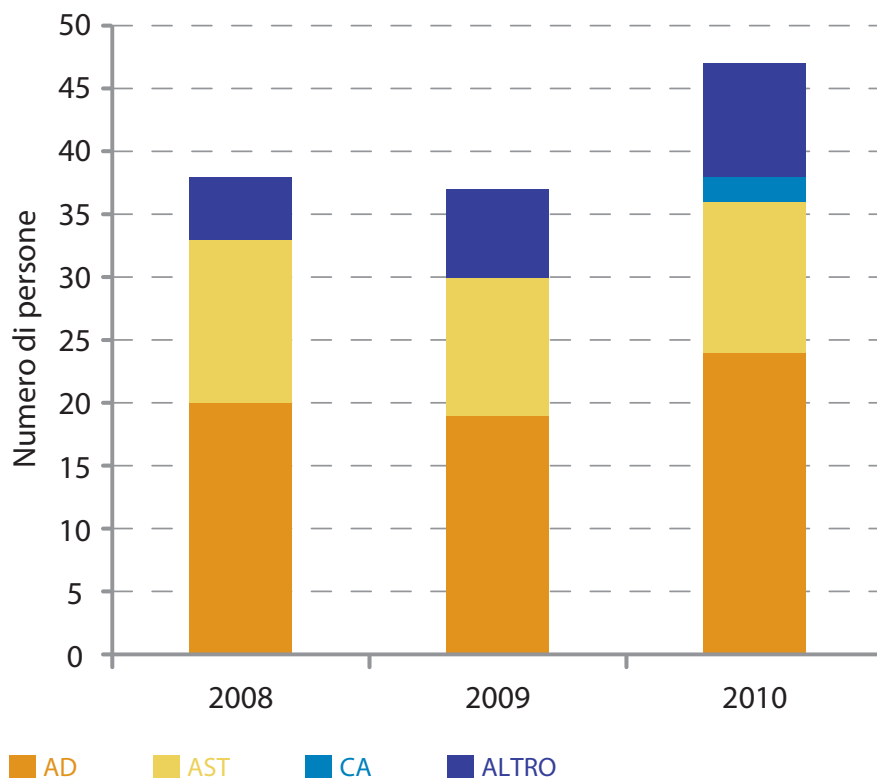
a luglio e da ottobre a febbraio). In via eccezionale e qualora siano soddisfatti severi criteri di ammissione, il GEPD può anche accogliere dottorandi per tirocinanti non retribuiti. Tutti i tirocinanti, remunerati e non, hanno contribuito all'attività sia teorica che pratica e hanno anche maturato utili esperienze di prima mano.

In base a un accordo sul livello dei servizi con la Commissione, il GEPD si è avvalso dell'assistenza amministrativa dell'Ufficio tirocini della direzione generale Istruzione e cultura della Commissione, che ha continuato a fornire un sostegno prezioso grazie alla vasta esperienza del proprio personale.

6.3.3. Programma per gli esperti nazionali distaccati

Il programma per gli esperti nazionali distaccati (END) è stato avviato nel gennaio 2006. In media sono stati distaccati ogni anno due esperti nazionali provenienti dalle autorità di protezione dei dati (APD) degli Stati membri. Grazie ai distacchi, il GEPD si è potuto avvalere delle competenze e dell'esperienza di queste persone e ha contribuito ad accrescere la propria visibilità a livello nazionale. Contemporaneamente, il programma consente agli esperti

Andamento del personale del GEPD per categoria



nazionali distaccati di familiarizzare con le tematiche relative alla protezione dei dati a livello comunitario.

6.3.4. Organigramma

L'organigramma del GEPD è rimasto invariato dal 2004 al 2009, quando sono state adottate le prime misure di riorganizzazione con la creazione del posto di direttore in qualità di responsabile del segretariato.

Nel 2010 l'organigramma ha subito profondi cambiamenti per effetto della riorganizzazione del personale in cinque settori – Controllo e applicazione delle norme, Politica e consulenza, Registrazione e supporto operativo, Informazione e comunicazione, Risorse umane, bilancio e amministrazione – i cui responsabili sono designati a livello amministrativo medio. Nell'ambito della nuova struttura organizzativa, il direttore rappresenta il GEPD in ambito amministrativo e assicura l'attuazione delle politiche e il coordinamento orizzontale delle attività. La responsabilità ultima della gestione rimane presso i Garanti, ma ora è maggiormente concentrata sull'elaborazione delle politiche e sulle relazioni interistituzionali.

Il risultato di questi cambiamenti è stato un nuovo organigramma, che è disponibile sul sito del GEPD.

6.3.5. Formazione

Offrire al personale migliori opportunità di formazione e di carriera è stata una delle priorità del 2010. È stato siglato un nuovo accordo sul livello dei servizi con il dipartimento Risorse umane della Commissione europea, che consente al GEPD l'accesso elettronico al catalogo formativo della Commissione dall'inizio del 2011. A partire da quella data, il personale del GEPD potrà infatti accedere direttamente al sistema di formazione SYSLOG e beneficiare delle stesse possibilità di formazione garantite ai funzionari della Commissione.

Molti dipendenti del GEPD hanno seguito corsi di lingua e partecipato agli eventi formativi organizzati a livello interistituzionale e, ove necessario, alla formazione esterna. Particolare successo ha ottenuto il corso "Programma di efficienza del personale (PEP)", organizzato specificamente per il GEPD. Nel 2010 sono stati coinvolti nelle attività di formazione tre settori, mentre nella prima metà del 2011 vi prenderanno parte tutti gli altri dipendenti.

Per effetto della riorganizzazione del GEPD, i nuovi dirigenti hanno ricevuto una specifica formazione

in campo amministrativo, sia a livello individuale che come gruppo.

Il GEPD ha continuato a essere presente nei comitati interistituzionali (Gruppo interistituzionale della Scuola europea di amministrazione (SEA), Gruppo interistituzionale di valutazione della formazione della SEA e Comitato interistituzionale per la formazione linguistica), che consentono di unire le forze e realizzare economie di scala in un'area in cui le esigenze sono sostanzialmente simili in tutte le istituzioni comunitarie. Come negli anni passati, il GEPD ha sottoscritto, insieme con altre istituzioni, il protocollo sull'armonizzazione dei costi dei corsi di lingua interistituzionali e il nuovo protocollo sulla distribuzione per istituzione dei costi dei progetti pedagogici sul linguaggio interistituzionale.

Nel 2011 il GEPD proseguirà gli sforzi volti a migliorare le opportunità di formazione e di carriera del proprio personale. È previsto inoltre un aggiornamento, in stretta consultazione con il personale, della decisione sulla formazione del 18 luglio 2007.

6.3.6. Attività sociali

Il GEPD ha firmato un accordo di cooperazione con la Commissione per agevolare l'integrazione dei nuovi assunti, ad esempio fornendo assistenza legale nelle questioni private (contratti di affitto, acquisto di una casa, eccetera) e offrendo l'opportunità di partecipare a varie attività sociali e di messa in rete. I nuovi assunti ricevono il personale benvenuto del Garante, del Garante aggiunto e del direttore del GEPD. Oltre ai rispettivi supervisori, incontrano anche i membri del settore Risorse umane, bilancio e amministrazione, che forniscono loro informazioni sulla gestione amministrativa e sulle procedure specifiche del GEPD.

Il GEPD ha continuato a sviluppare la cooperazione interistituzionale per quanto riguarda la custodia dei bambini: i figli dei dipendenti del GEPD hanno accesso agli asili nido, ai doposcuola e ai centri di custodia all'aperto della Commissione, come pure alle Scuole europee. Il GEPD partecipa inoltre, in qualità di osservatore, al comitato consultivo del Parlamento europeo sulla prevenzione e protezione nei luoghi di lavoro, che ha lo scopo di migliorare gli ambienti di lavoro.

Nel 2010 i nuovi settori creati all'interno del GEPD hanno organizzato le "Giornate fuori dall'ufficio", per promuovere lo spirito di gruppo e favorire l'integrazione dei nuovi arrivati. Alla fine dell'anno si è tenuto un incontro conviviale del personale in

occasione delle feste natalizie, che ha offerto l'occasione di accogliere i nuovi colleghi e di fare il bilancio di un anno intenso e ricco di cambiamenti.

6.4. Funzioni di controllo

6.4.1. Controllo interno

Il sistema di controllo interno, in vigore dal 2006, assicura il conseguimento degli obiettivi del GEPD in maniera efficiente e in conformità delle norme e dei regolamenti. Il GEPD ha adottato procedure di controllo interno specifiche e rispondenti alle sue esigenze, dimensioni e attività. Il sistema è stato progettato per poter gestire, anziché eliminare, il rischio di mancato raggiungimento degli obiettivi istituzionali.

Il GEPD ha preso atto della relazione annuale di attività e della dichiarazione di affidabilità firmate dall'ordinatore delegato. Nel complesso, il GEPD ritiene che i sistemi di controllo interno in atto forniscano ragionevoli garanzie quanto alla liceità e regolarità delle operazioni delle quali è responsabile. Nondimeno, nel 2010 è stato adottato un approccio più ambizioso. L'elenco delle azioni che applicano gli standard del controllo interno è stato ampliato, per garantire un più efficiente controllo interno dei processi.

Ad esempio, sono stati adottati nuovi manuali per una migliore gestione dei processi, come quelli relativi ai controlli preventivi, ai reclami e ai procedimenti giudiziari. Sono in fase di elaborazione, in stretta consultazione con il personale e con il pieno sostegno dei Garanti, alcune attività come le azioni di sensibilizzazione in materia di etica, l'introduzione di descrizioni più dettagliate dei posti di lavoro, l'adozione di norme interne aggiuntive e di un nuovo sistema di tutoraggio.

6.4.2. Audit interno

Il revisore interno della Commissione è stato nominato revisore interno anche del GEPD. Al fine di assicurare una gestione efficace delle risorse del GEPD, il revisore interno effettua controlli periodici dei sistemi di controllo interno e delle operazioni finanziarie del GEPD.

In riferimento alla verifica di follow-up eseguita nel dicembre 2008 dal servizio di audit interno, una relazione adottata nel maggio 2009 ha confermato il conseguimento degli obiettivi del GEPD, ma ha anche individuato taluni punti che possono essere migliorati. Su alcuni di essi si è già intervenuto,

mentre gli altri sono sottoposti a revisione nel contesto della riorganizzazione del GEPD.

È stato programmato per l'inizio del 2011 un esercizio di valutazione da parte del servizio di audit interno, in vista di una verifica nei mesi successivi.

6.4.3. Sicurezza

Nel dicembre 2010 il GEPD ha deciso di affidare a due dei propri dipendenti le funzioni di responsabile e responsabile aggiunto locale della sicurezza nonché di responsabile e responsabile aggiunto locale della sicurezza delle informazioni. In entrambi i casi, gli incarichi sono stati assegnati a tempo parziale. Sono stati avviati i primi contatti con i servizi della Commissione europea e del Parlamento europeo ed è stato concordato un primo ambito di cooperazione. È iniziato il processo di concessione del nulla osta di sicurezza per il personale interessato e saranno intraprese altre azioni concernenti la sicurezza delle informazioni e la sicurezza delle tecnologie informatiche, con particolare riguardo allo sviluppo del sistema interno di gestione dei casi del GEPD.

Nel 2011 il GEPD continuerà a operare conformemente alla decisione sulla sicurezza adottata alla fine del 2008, che prevede misure di gestione delle informazioni riservate e della sicurezza delle tecnologie informatiche e stabilisce le condizioni di salute e di sicurezza per il personale e i locali.

6.5. Infrastrutture

In virtù dell'accordo di cooperazione amministrativa, il GEPD ha sede nei locali del Parlamento europeo, che gli fornisce anche assistenza per quanto attiene alle tecnologie dell'informazione e alle infrastrutture. Visto il considerevole aumento del personale nel 2010, il Parlamento europeo ha messo a disposizione del GEPD nuovi spazi.

L'edificio che ospita il GEPD è stato in parte rinnovato nel 2010. I relativi lavori, eseguiti sotto la supervisione del Parlamento europeo, hanno reso gli ambienti di lavoro molto più confortevoli e piacevoli. Tuttavia, la carenza di spazi rimane un motivo di grave preoccupazione per il GEPD e tale questione è stata oggetto di diversi incontri con il Parlamento europeo.

L'istituzione ha continuato a gestire autonomamente l'inventario del mobilio e delle dotazioni informatiche, con l'aiuto dei servizi del Parlamento europeo.

6.6. Contesto amministrativo

6.6.1. Assistenza amministrativa e cooperazione interistituzionale

Il GEPD si avvale della cooperazione interistituzionale in molti settori, in conformità dell'accordo stipulato nel 2004 con i segretariati generali della Commissione, del Parlamento e del Consiglio. L'accordo è stato prorogato nel 2006 (per un triennio) e nel 2010 (per un biennio). Questa cooperazione è d'importanza vitale per il GEPD perché aumenta l'efficienza e consente economie di scala.

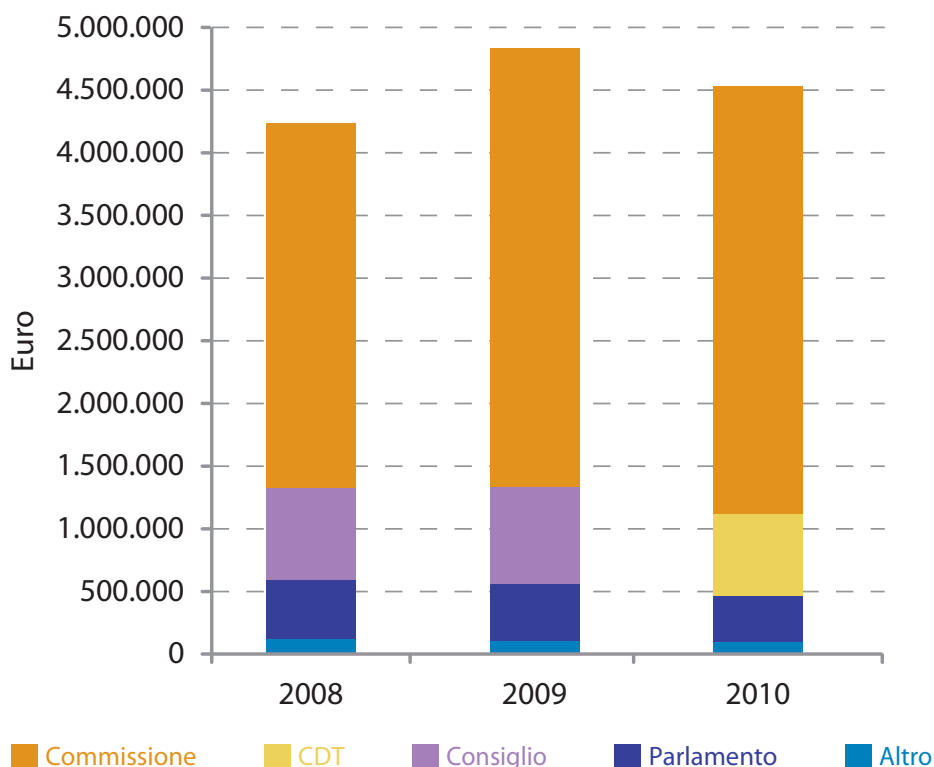
Nel 2010 è proseguita la cooperazione interistituzionale con varie direzioni generali della Commissione (Personale e amministrazione, Bilancio, Servizio di audit interno, Istruzione e cultura), l'Ufficio di gestione e liquidazione dei diritti individuali, la Scuola europea di amministrazione e vari servizi del Parlamento europeo (servizi informatici, in particolare attraverso accordi per la manutenzione e lo sviluppo del sito Internet del GEPD, attrezzature per i locali, sicurezza dell'edificio, stampa, posta elettronica, telefoni, provviste, eccetera). In molti casi, la cooperazione avviene sulla base di accordi sul livello dei servizi, periodicamente aggiornati. Il

GEPD ha inoltre continuato a partecipare agli inviti interistituzionali a presentare proposte, contribuendo così all'efficienza in molti ambiti amministrativi e acquisendo maggiore autonomia.

L'accordo con il Consiglio europeo sui servizi di traduzione è scaduto nel gennaio 2010. È stato siglato un nuovo accordo con il Centro di traduzione degli organismi dell'Unione europea, che ha assunto l'attività di traduzione a partire dal 2010.

Il GEPD è membro di numerosi comitati e gruppi di lavoro interistituzionali, tra cui il Collegio dei capi dell'amministrazione, il *Comité de Gestion Assurances maladies*, il *Comité de Préparation pour les Questions Statutaires*, il *Comité du Statut*, il Gruppo di lavoro interistituzionale/Scuola europea di amministrazione, il consiglio di amministrazione dell'EPSO, il Gruppo di lavoro dell'EPSO e la *Commission paritaire commune*. Il GEPD è membro anche del *Comité de préparation pour les affaires sociales* e partecipa al suo gruppo ad hoc che si occupa dell'applicazione nelle istituzioni europee della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità. Queste partecipazioni hanno contribuito ad accrescere la visibilità del GEPD tra le altre istituzioni e hanno incoraggiato la condivisione di buone pratiche.

GEPD – esecuzione del bilancio attraverso la cooperazione interistituzionale



6.6.2. Norme interne

È proseguito il processo di adozione di norme interne per assicurare il corretto funzionamento del GEPD. Negli ambiti nei quali il GEPD beneficia dell'assistenza della Commissione o del Parlamento europeo, le norme sono simili a quelle delle altre istituzioni, sia pure con alcune differenze dovute alle caratteristiche specifiche dell'ufficio del GEPD.

Il GEPD è un'istituzione relativamente giovane e si sta sviluppando rapidamente. Di conseguenza, le norme e le procedure che erano appropriate nei suoi primi anni di attività possono rivelarsi meno efficaci in momenti successivi, a fronte di una struttura più grande e più complessa. Le norme sono pertanto soggette a valutazione e nei prossimi anni potrebbero essere modificate. L'opera di valutazione è iniziata nel 2010 in vista di una modifica del codice di condotta del GEPD.

6.6.3. Gestione dei documenti

Con il sostegno dei servizi del Parlamento europeo, nel 2009 è stato applicato con successo un nuovo sistema di gestione della posta elettronica (GEDA) per le attività amministrative. Dopo questa prima fase, sono stati condotti studi per individuare un sistema adeguato di gestione dei documenti e dei fascicoli per il dipartimento di protezione dei dati.

Nel corso del 2010 sono stati definiti in dettaglio una serie di requisiti istituzionali per l'elaborazione di un adeguato sistema di gestione dei documenti e delle registrazioni, compresa la gestione dei fascicoli. Consulenti esterni sono stati incaricati di eseguire un'analisi di mercato nell'ottica di individuare idonee soluzioni potenziali. La direzione generale Innovazione e supporto tecnologico del Parlamento europeo (ITEC) continua a sostenere e affiancare il GEPD in questo processo. È stato costituito un gruppo di progetto interno, guidato dal responsabile del settore Registrazione e supporto operativo. Di questo gruppo multidisciplinare fanno parte rappresentanti di cinque settori.

Parallelamente a tali sviluppi in campo tecnologico, il settore Registrazione e supporto tecnologico ha continuato a garantire un'accurata gestione delle registrazioni. È stato adottato un piano di compilazione per quattro dei cinque settori e sono state semplificate le procedure per la registrazione della posta, tenendo conto della

nuova struttura organizzativa del GEPD. Particolare attenzione è stata riservata ai requisiti di rendicontazione dell'amministrazione del GEPD. Le informazioni specifiche dei fascicoli sono state individuate e raccolte da tutti i settori, per migliorare la tracciabilità dei fascicoli.

7

IL RESPONSABILE DELLA PROTEZIONE DEI DATI PRESSO IL GEPD

7.1. Un nuovo gruppo dell'RPD presso il GEPD

Come tutte le altre istituzioni europee, anche il GEPD è tenuto a rispettare determinati obblighi giuridici per quanto attiene alla protezione dei dati personali. Tali obblighi sono stabiliti dal regolamento sulla protezione dei dati (regolamento (CE) n. 45/2001).

Oltre a specificare i principi giuridici che disciplinano il trattamento dei dati personali da parte dell'amministrazione comunitaria, il regolamento prevede che ciascuna istituzione o organismo dell'Unione europea nomini almeno un responsabile della protezione dei dati (RPD).

Nel settembre 2010 il GEPD ha designato un **nuovo RPD** e anche un **RPD aggiunto**. In tal modo il GEPD investe nuove energie per conseguire rapidamente un più alto grado di conformità.

Il ruolo dell'RPD presso il GEPD comporta molte sfide, quali: essere indipendente all'interno di un'istituzione indipendente, soddisfare le elevate aspettative di colleghi particolarmente attenti e sensibili alle questioni correlate alla protezione dei dati e trovare soluzioni in grado di fungere da riferimento per altre istituzioni.

7.2. Piano d'azione e norme di applicazione

Il gruppo dell'RPD recentemente istituito ha inviato al personale un **piano d'azione** generale e le relative priorità. Il piano d'azione individua quattro aree principali alle quali il gruppo dell'RPD intende dare forte enfasi: aspetti organizzativi, funzione consultiva, informazione e sensibilizzazione.

Un primo passo importante è stata l'adozione delle **norme di applicazione dell'RPD** nell'ottobre 2010. Tali norme si rifanno a quelle di altre istituzioni nonché agli orientamenti del Garante, adeguandoli alle peculiarità del GEPD. Per esempio, la garanzia che l'RPD può essere licenziato solamente previo consenso del GEPD è stata modificata per prevedere il consenso sia del Garante che del Garante aggiunto. Inoltre, in riferimento al documento sugli standard dell'RPD, le norme di applicazione sottolineano la necessità di una buona conoscenza della protezione dei dati, nonché di autonomia nel processo di rendicontazione.

7.3. Un registro delle operazioni di trattamento facilmente accessibile

Il gruppo dell'RPD ha eseguito un accurato controllo dell'**inventario delle operazioni di trattamento esistenti** e ha richiamato l'attenzione del personale sull'esigenza di garantire che tutte le operazioni di trattamento presso il GEPD siano

notificate. A tal fine, ai responsabili del trattamento è stato chiesto di preparare le notifiche mancanti. Il gruppo dell'RPD ha anche fornito assistenza, ove necessario, per la preparazione di notifiche nuove e il completamento di quelle pendenti.

È stata messa a disposizione online una versione elettronica del registro delle operazioni di trattamento. Grazie a un collegamento con tutte le notifiche finali, tale versione consente un facile accesso a chiunque intenda consultare il registro, in conformità dell'articolo 26 del regolamento sulla protezione dei dati.

Il gruppo dell'RPD ha inoltre aggiornato e migliorato i moduli di notifica del trattamento di dati personali all'interno del segretariato del GEPD.

7.4. Esercizio di primavera

Il gruppo dell'RPD ha dato seguito all'ultimo "esercizio di primavera" (cfr. sezione 2.5.2) fornendo al GEPD informazioni aggiornate sulla conformità della protezione dei dati all'interno dell'istituzione. La lettera inviata al GEPD all'inizio del 2011 metteva in evidenza i risultati conseguiti e sottolineava l'intenzione, in linea con il piano d'azione dell'RPD, di migliorare la conformità e la consapevolezza della protezione dei dati, particolarmente nel settore delle risorse umane.

7.5. Informazione e sensibilizzazione

Il gruppo dell'RPD attribuisce grande importanza alla sensibilizzazione e alla comunicazione sul tema della conformità del GEPD alle norme in materia di protezione dei dati, sia esternamente che internamente.

Per quanto attiene alla **comunicazione esterna**, sul sito Internet del GEPD è ora disponibile una sezione dedicata all'RPD che fornisce informazioni di base sul ruolo e sulle attività dell'RPD. Sono disponibili online anche le norme di applicazione e il registro delle operazioni di trattamento del GEPD.

Inoltre, il gruppo dell'RPD ha partecipato alle **riunioni della rete di RPD**, che costituiscono un'eccellente occasione per confrontarsi con i colleghi, discutere problematiche comuni e condividere le migliori pratiche. Il gruppo dell'RPD ha anche

svolto un ruolo attivo nelle attività organizzate in occasione della Giornata della protezione dei dati.

Quanto alla **comunicazione interna**, l'Intranet istituita di recente rappresenta una grande opportunità per comunicare con i dipendenti. La sezione Intranet dell'RPD contiene informazioni utili per il personale riguardanti gli aspetti principali del ruolo dell'RPD, le norme di applicazione e il piano d'azione dell'RPD, nonché informazioni sulle sue attività. Il gruppo dell'RPD intende altresì utilizzare questo spazio virtuale per accrescere la visibilità delle informazioni che saranno fornite agli interessati, ai sensi degli articoli 11 e 12 del regolamento. A tale proposito, il gruppo dell'RPD ha cominciato a mettere a disposizione su Intranet riferimenti alle dichiarazioni sulla tutela della vita privata concernenti le operazioni di trattamento in corso presso il GEPD, allo scopo di renderle più facilmente accessibili per tutto il personale.

8

PRINCIPALI OBIETTIVI PER IL 2011

Per il 2011 sono stati scelti gli obiettivi indicati di seguito. Dei risultati conseguiti si darà conto l'anno prossimo.

8.1. Controllo e applicazione della legge

In linea con il documento politico sulla conformità e l'applicazione della legge adottato nel dicembre 2010, il GEPD ha fissato i seguenti obiettivi nel campo del controllo e dell'applicazione della legge.

- **Sensibilizzazione**

Il GEPD continuerà a investire tempo e risorse per fornire consulenza e orientamenti sulle tematiche riguardanti la protezione dei dati. Quest'opera di sensibilizzazione sarà concretizzata mediante documenti di orientamento su temi selezionati nonché attraverso seminari o laboratori interattivi durante i quali il GEPD illustrerà la propria posizione su una determinata questione.

- **Ruolo dei controlli preventivi**

Considerato che è stato quasi del tutto smaltito l'arretrato dei controlli preventivi ex post, il GEPD si concentrerà sull'analisi delle conseguenze delle nuove operazioni di trattamento e continuerà a riservare particolare attenzione all'attuazione delle raccomandazioni formulate nei pareri su controlli preventivi, nonché a garantire un seguito adeguato.

- **Esercizi di monitoraggio e rendicontazione**

Il GEPD continuerà a monitorare l'applicazione delle norme e dei principi sulla protezione dei dati da parte delle istituzioni e degli organismi interessati attraverso sia un esercizio generale di monitoraggio (primavera 2011) sia esercizi mirati di monitoraggio quando il livello di conformità presso determinate istituzioni o organismi sia preoccupante.

- **Ispezioni**

Il GEPD procederà a ispezioni in loco nei casi in cui abbia validi motivi di ritenere che il meccanismo di conformità sia bloccato. Le ispezioni saranno considerate l'ultimo atto prima di ricorrere ad azioni formali di applicazione della legge. Ispezioni e audit saranno attuati anche nell'ambito dei sistemi informatici su larga scala che rientrano nella sfera di competenza del GEPD.

8.2. Politica e consultazione

Gli obiettivi principali sono conformi alle priorità fissate per quest'area per il 2011, come pubblicato sul sito Internet. Inoltre, sono stati definiti obiettivi di cooperazione con le autorità di protezione dei dati e per il controllo coordinato dei sistemi informatici su larga scala.

- **Ambito della consultazione**

Il GEPD continuerà a formulare in modo tempestivo pareri e osservazioni su proposte di nuovi atti legislativi e ad assicurare un seguito adeguato in tutti

i campi rilevanti. Particolare attenzione sarà riservata, come specificato prima, alla revisione del quadro giuridico, all'attuazione del programma di Stoccolma e a iniziative nell'area della tecnologia.

- **Revisione del quadro giuridico**

Il GEPD considera prioritaria l'elaborazione di un quadro giuridico complessivo per la protezione dei dati. Emetterà un parere legislativo sulla comunicazione della Commissione relativa all'approccio globale alla protezione dei dati personali, nonché su ogni altra proposta legislativa successiva, e contribuirà al dibattito ove necessario e opportuno.

- **Attuazione del programma di Stoccolma**

Il GEPD continuerà a dedicare speciale attenzione alle varie iniziative concernenti la prosecuzione dell'attuazione del programma di Stoccolma nello spazio di libertà, sicurezza e giustizia, come l'istituzione di un sistema a entrata-uscita e il programma per viaggiatori registrati, la prevista direttiva sull'utilizzo dei dati del codice di prenotazione a fini di applicazione della legge e l'introduzione di un TFTP europeo.

- **Iniziative nel campo della tecnologia**

Nel 2011 il GEPD seguirà da vicino anche le iniziative nel campo della tecnologia che possono avere un impatto sulla protezione della vita privata e dei dati. In particolare, il GEPD continuerà a monitorare l'applicazione delle componenti informatiche di Europa 2020 nell'ambito dell'agenda digitale, come l'identificazione a radiofrequenza, il cloud computing, il governo elettronico e l'applicazione online dei diritti di proprietà intellettuale.

- **Altre iniziative**

Il GEPD si concentrerà su tutte le altre iniziative che possono avere significative conseguenze sulla protezione dei dati, come quelle nel settore dei trasporti (ad esempio, l'impiego di body scanner negli aeroporti, pacchetti di mobilità elettronica) e gli scambi di dati su larga scala che possono avvenire nel sistema d'informazione del mercato interno.

- **Cooperazione con le autorità di protezione dei dati**

Il GEPD continuerà a contribuire attivamente alle attività e al successo del gruppo di lavoro Articolo 29 sulla protezione dei dati intervenendo sul suo programma di lavoro in conformità delle priorità del GEPD, garantendo coerenza e sinergie tra il gruppo di

lavoro e le posizioni del GEPD e intrattenendo rapporti costruttivi con le autorità nazionali di protezione dei dati. In qualità di relatore per fascicoli specifici, il GEPD guiderà e preparerà l'adozione dei pertinenti pareri del gruppo di lavoro Articolo 29.

- **Controllo coordinato**

La normativa comunitaria prescrive il controllo coordinato di Eurodac, il sistema d'informazione doganale, e, dalla metà del 2011, del sistema d'informazione sui visti. Un obiettivo importante del GEPD sarà quello di dotare di un segretariato efficiente le autorità di protezione dei dati che partecipano al controllo coordinato. In qualità di controllore dei sistemi informatici su larga scala, il GEPD parteciperà attivamente anche al loro controllo coordinato ed effettuerà audit periodici di sicurezza.

8.3. Altri campi

- **Informazione e comunicazione**

L'informazione, la comunicazione e le attività destinate ai media continueranno a essere sviluppate e migliorate, con un'attenzione speciale per l'opera di sensibilizzazione, le pubblicazioni e l'informazione online. Inoltre, il GEPD preparerà il terreno per una revisione della strategia di comunicazione, in consultazione con le parti interessate più importanti. Questo esercizio generale sarà accompagnato da valutazioni più mirate dell'impatto dei principali strumenti d'informazione e comunicazione.

- **Organizzazione interna**

I principali obiettivi per il 2011 saranno il completamento della riorganizzazione interna, un impegno rinnovato per la gestione della prestazione nel contesto di una revisione strategica e lo sviluppo e l'applicazione di nuovi strumenti informatici. Particolare attenzione sarà riservata al controllo e alle procedure interne, a una migliore destinazione delle risorse e a una migliore esecuzione del bilancio.

- **Gestione delle risorse**

Il GEPD continuerà a investire risorse nello sviluppo e nell'applicazione di un sistema di gestione dei fascicoli. Priorità sarà data alla conclusione di accordi sul livello dei servizi con la Commissione europea riguardo all'impiego di applicazioni informatiche nel settore delle risorse umane (ad esempio, Syslog Formazione, Sysper e i sistemi di trattamento per le missioni).

Allegato A — Quadro giuridico

L'articolo 286 del trattato CE, adottato nel 1997 come parte del trattato di Amsterdam, prevedeva che gli atti comunitari sulla protezione delle persone fisiche riguardanti il trattamento dei dati personali e la libera circolazione di tali dati si applicassero anche alle istituzioni e agli organismi comunitari, e che fosse istituito un organo di controllo indipendente.

Gli atti comunitari cui fa riferimento tale disposizione sono la direttiva 95/46/CE, che prevede un quadro generale per la normativa in materia di protezione dei dati negli Stati membri, e la direttiva 97/66/CE, specifica di un settore, sostituita poi dalla direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche. Entrambe le direttive possono essere considerate il risultato di uno sviluppo giuridico iniziato nei primi anni '70 all'interno del Consiglio d'Europa (cfr. più sotto).

Sulla base dell'articolo 286 del trattato CE, il Garante europeo della protezione dei dati è stato istituito dal regolamento (CE) n. 45/2001 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, entrato in vigore nel 2001⁽²³⁾. Il regolamento stabilisce inoltre norme specifiche per le istituzioni e gli organismi in linea con le due direttive.

Dopo l'entrata in vigore del trattato di Lisbona, il suddetto articolo 286 è stato sostituito dall'articolo 16 del trattato sul funzionamento dell'Unione europea, che sottolinea l'importanza della protezione dei dati personali in termini più generali. Sia l'articolo 16 TFUE che l'articolo 8 della Carta dei diritti fondamentali dell'UE, attualmente vincolante, stabiliscono che la conformità alle norme sulla protezione dei dati deve essere soggetta al controllo di un'autorità indipendente.

Antecedenti

L'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali prevede il diritto al rispetto della vita privata e della vita familiare, fatte salve alcune restrizioni che sono ammesse solo a determinate condizioni. Tuttavia, nel 1981 si è ritenuto necessario adottare una convenzione distinta sulla protezione dei dati, al fine

di sviluppare un approccio positivo e strutturale alla tutela dei diritti e delle libertà, tenendo conto delle possibili influenze del trattamento dei dati personali in una società moderna. Tale convenzione, nota anche come Convenzione 108, è stata ratificata da oltre 40 paesi appartenenti al Consiglio d'Europa, compresi tutti gli Stati membri dell'UE.

La direttiva 95/46/CE era basata sui principi della Convenzione 108, che ha tuttavia specificato e rielaborato sotto molti aspetti. Lo scopo era di fornire un elevato grado di tutela e garantire la libera circolazione dei dati personali nell'UE. Presentando la proposta di questa direttiva, all'inizio degli anni '90, la Commissione dichiarò che le istituzioni e gli organismi comunitari dovevano beneficiare di analoghe garanzie giuridiche, che consentissero loro di partecipare alla libera circolazione dei dati personali, sulla base di norme di protezione equivalenti. Però, fino all'adozione dell'articolo 286 del trattato CE, mancava una base giuridica per un siffatto regime.

Il trattato di Lisbona, entrato in vigore il 1° dicembre 2009, rafforza in vari modi la tutela dei diritti fondamentali. Il rispetto della vita privata e della vita familiare nonché la protezione dei dati personali sono considerati diritti fondamentali distinti negli articoli 7 e 8 della Carta, che è diventata giuridicamente vincolante sia per le istituzioni e gli organi comunitari sia per gli Stati membri dell'UE nell'applicazione del diritto comunitario. La protezione dei dati è contemplata come questione orizzontale anche dall'articolo 16 TFUE. Questa è una chiara dimostrazione del fatto che la protezione dei dati è vista come un elemento basilare del "buon governo". Il controllo indipendente è un fattore essenziale di tale protezione.

Regolamento (CE) n. 45/2001

Ad un esame attento andrebbe innanzi tutto rilevato che, ai sensi dell'articolo 3, paragrafo 1, il regolamento si applica "al trattamento di dati personali da parte di tutte le istituzioni e di tutti gli organismi comunitari, nella misura in cui detto trattamento avviene nell'esercizio di attività che rientrano in tutto o in parte nel campo di applicazione del diritto comunitario". Ma, con l'entrata in vigore del trattato di Lisbona e la conseguente abolizione della struttura a pilastri – per effetto della quale i riferimenti alle "istituzioni comunitarie" e al "diritto comunitario" non sono più validi –, il regolamento vale, in linea di principio, per tutte le istituzioni e gli organismi comunitari, ove non diversamente previsto in modo specifico da altri atti comunitari. Le precise implicazioni di que-

⁽²³⁾ GU L 8 del 12.1.2001, pag. 1.

sti cambiamenti sono ancora oggetto di scrutinio e possono necessitare di ulteriori chiarimenti.

Le definizioni e la sostanza del regolamento seguono da vicino l'approccio della direttiva 95/46/CE. Si potrebbe affermare che il regolamento (CE) n. 45/2001 rappresenta l'attuazione della direttiva a livello europeo. Ciò significa che il regolamento riguarda principi generali, quali il trattamento lecito e corretto, la proporzionalità e l'uso compatibile, le categorie particolari di dati sensibili, le informazioni da fornire agli interessati, i diritti degli interessati, gli obblighi dei responsabili del trattamento – tenendo conto, se del caso, di circostanze speciali a livello di Unione europea – nonché il controllo, l'attuazione e i mezzi di ricorso. Un capo distinto riguarda la protezione dei dati personali e la tutela della vita privata nell'ambito delle reti interne di telecomunicazione, e rappresenta l'attuazione a livello europeo della direttiva 97/66/CE sulla tutela della vita privata nel settore delle telecomunicazioni.

Caratteristica interessante del regolamento è l'obbligo imposto alle istituzioni e agli organismi comunitari di designare almeno un responsabile della protezione dei dati (RPD) con il compito di garantire in maniera indipendente l'applicazione interna delle disposizioni del regolamento, compresa la corretta notifica dei trattamenti. Tutte le istituzioni comunitarie e la maggior parte degli organismi hanno ora un responsabile della protezione dei dati, in alcuni casi già da vari anni. Ciò significa che è stato svolto un lavoro considerevole per applicare il regolamento anche in mancanza di un organismo di controllo. I responsabili della protezione dei dati possono anche trovarsi in una posizione migliore per fornire pareri o intervenire tempestivamente e per contribuire all'elaborazione di buone pratiche. Poiché hanno l'obbligo formale di collaborare con il GEPD, si è creata una rete molto importante e altamente apprezzata che consente di operare assieme con la prospettiva di ulteriori sviluppi (cfr. sezione 2.2).

Compiti e poteri del GEPD

I compiti e i poteri del GEPD sono descritti chiaramente negli articoli 41, 46 e 47 del regolamento (cfr. allegato B), sia in termini generici che in termini specifici. L'articolo 41 enuncia il mandato generale del GEPD: garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, riguardo al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari. Espone inoltre per sommi capi alcuni elementi specifici di tale mandato. Queste

responsabilità generali sono sviluppate e specificate negli articoli 46 e 47 in forma di un elenco particolareggiato di funzioni e competenze.

La descrizione delle responsabilità, delle funzioni e delle competenze segue essenzialmente lo stesso modello previsto per gli organi di controllo nazionali: gestire i reclami e compiere i relativi accertamenti, svolgere altre indagini, informare i responsabili del trattamento e gli interessati, effettuare controlli preventivi in caso di trattamenti che presentano rischi specifici, eccetera. Il regolamento conferisce al GEPD il potere di accedere alle informazioni e ai locali pertinenti, qualora ciò sia necessario ai fini delle indagini. Il Garante può anche imporre sanzioni e adire la Corte di giustizia. Queste attività di controllo sono trattate in modo più ampio nel capitolo 2 della presente relazione.

Alcune funzioni sono di natura particolare. Il compito di fornire pareri alla Commissione e alle altre istituzioni sui nuovi atti legislativi — ribadito all'articolo 28, paragrafo 2, dall'obbligo formale imposto alla Commissione di consultare il GEPD al momento dell'adozione di una proposta legislativa relativa al trattamento di dati personali — si riferisce anche alle proposte di direttive e alle altre misure destinate a essere applicate a livello nazionale o recepite nel diritto nazionale. Si tratta di una funzione strategica che consente al GEPD di valutare in una fase precoce le implicazioni in materia di tutela della vita privata e di discutere possibili alternative, anche riguardo alle questioni che rientrano nell'ex "terzo pilastro" (cooperazione di polizia e giudiziaria in materia penale). Altri compiti importanti sono il controllo degli sviluppi rilevanti che possono avere ripercussioni sulla protezione dei dati personali e gli interventi nei procedimenti davanti alla Corte di giustizia. Per approfondimenti su queste attività consultive del GEPD si rimanda al capitolo 3 della presente relazione.

Ripercussioni analoghe comporta l'obbligo di collaborare con le autorità nazionali di controllo e gli organi di controllo nelle materie dell'ex "terzo pilastro". In qualità di membro del gruppo di lavoro Articolo 29 per la tutela dei dati, istituito per fornire pareri alla Commissione europea e sviluppare politiche armonizzate, il GEPD ha la possibilità di fornire il proprio contributo a tale livello. La collaborazione con gli organi di controllo nell'ambito dell'ex terzo pilastro gli consente di seguire gli sviluppi in tale contesto e di contribuire a un quadro più coerente e uniforme per quanto riguarda la protezione dei dati personali, a prescindere dal pilastro o dal contesto specifico. Tale collaborazione è trattata più approfonditamente nel capitolo 4 della presente relazione.

Allegato B — Estratto dal regolamento (CE) n. 45/2001

Articolo 41 — Garante europeo della protezione dei dati

1. È istituita un'autorità di controllo indipendente denominata garante europeo della protezione dei dati.
2. Il garante europeo della protezione dei dati ha il compito di garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, riguardo al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari.

Il garante europeo della protezione dei dati ha il compito di sorvegliare e assicurare l'applicazione del presente regolamento e di qualunque altro atto comunitario relativo alla tutela dei diritti e delle libertà fondamentali delle persone fisiche riguardo al trattamento dei dati personali da parte di un'istituzione o di un organismo comunitario, e di fornire alle istituzioni e agli organismi comunitari nonché agli interessati pareri su tutte le questioni relative al trattamento dei dati personali. A tal fine esso assolve agli obblighi previsti all'articolo 46 ed esercita i poteri attribuitigli dall'articolo 47.

Articolo 46 — Funzioni

Il garante europeo della protezione dei dati assolve i seguenti compiti:

- a) tratta i reclami e compie i relativi accertamenti, e ne comunica l'esito agli interessati entro un termine ragionevole;
- b) svolge indagini di propria iniziativa o in seguito a un reclamo e ne comunica l'esito agli interessati entro un termine ragionevole;
- c) sorveglia e garantisce l'applicazione del presente regolamento e di qualunque altro atto comunitario relativo alla tutela delle persone fisiche riguardo al trattamento dei dati personali da parte di un'istituzione o di un organismo comunitario, fatta eccezione per la Corte di giustizia delle Comunità europee nell'esercizio delle sue funzioni giurisdizionali;

- d) consiglia le istituzioni e gli organismi comunitari, di propria iniziativa o su richiesta, in ordine a qualsiasi argomento relativo al trattamento di dati personali, in particolare prima che essi adottino regolamentazioni interne relative alla tutela dei diritti e delle libertà fondamentali riguardo al trattamento di dati personali;
- e) sorveglia l'evoluzione delle tecnologie che presentano un interesse, se ed in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione;
- f) collabora con le autorità nazionali di controllo di cui all'articolo 28 della direttiva 95/46/CE dei paesi cui si applica tale direttiva se ed in quanto ciò risulti necessario per l'adempimento dei rispettivi obblighi, in particolare scambiando ogni informazione utile, chiedendo a dette autorità o organi di esercitare le loro funzioni o rispondendo a loro richieste; ii) collabora altresì con gli organi di controllo della protezione dei dati istituiti in virtù del titolo VI del trattato sull'Unione europea, in particolare per rendere più coerente l'applicazione delle norme e procedure che sono rispettivamente incaricati di fare osservare;
- g) partecipa alle attività del «Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali», istituito dall'articolo 29 della direttiva 95/46/CE;
- h) determina, motiva e rende pubbliche le deroghe, le garanzie, le autorizzazioni e le condizioni di cui all'articolo 10, paragrafo 2, lettera b), paragrafi 4, 5 e 6, all'articolo 12, paragrafo 2, all'articolo 19 e all'articolo 37, paragrafo 2;
- i) tiene un registro dei trattamenti notificatigli ai sensi dell'articolo 27, paragrafo 2, e registrati a norma dell'articolo 27, paragrafo 5, e fornisce i mezzi necessari per accedere ai registri tenuti dai responsabili della protezione dei dati a norma dell'articolo 26;
- j) procede ad un esame preventivo dei trattamenti notificatigli;
- k) adotta il proprio regolamento interno.

Articolo 47 — Competenze

1. Il garante europeo della protezione dei dati può:

- a) offrire consulenza agli interessati nell'esercizio dei loro diritti;
- b) rivolgersi al responsabile del trattamento in caso di asserita violazione delle disposizioni sul trattamento dei dati personali e, all'occorrenza, presentare proposte volte a porre rimedio a tale violazione e a migliorare la protezione degli interessati;
- c) ordinare che siano soddisfatte le richieste di esercizio di determinati diritti allorché dette richieste siano state respinte in violazione degli articoli da 13 a 19;
- d) rivolgere avvertimenti o moniti al responsabile del trattamento;
- e) ordinare la rettifica, il blocco, la cancellazione o la distruzione di tutti i dati che siano stati trattati in violazione delle disposizioni sul trattamento dei dati personali e la notificazione di misure ai terzi ai quali i dati sono stati comunicati;
- f) vietare trattamenti a titolo provvisorio o definitivo;
- g) adire l'istituzione o l'organismo comunitario in questione e, se necessario, il Parlamento europeo, il Consiglio e la Commissione;
- h) adire la Corte di giustizia delle Comunità europee alle condizioni previste dal trattato;
- i) intervenire nelle cause dinanzi alla Corte di Giustizia delle Comunità europee.

2. Il garante europeo della protezione dei dati ha il potere di:

- a) ottenere da un responsabile del trattamento o da un'istituzione o un organismo comunitario l'accesso a tutti i dati personali e a tutte le informazioni necessarie alle sue indagini;
- b) accedere a tutti i locali in cui un responsabile del trattamento o un'istituzione o un organismo comunitario svolge le sue attività se si può ragionevolmente supporre che in essi viene svolta un'attività in applicazione del presente regolamento.

Allegato C — Elenco delle abbreviazioni

ACTA	Accordo commerciale anticontraffazione	END	Esperto nazionale distaccato
APD	Autorità di protezione dei dati	ENISA	Agenzia europea per la sicurezza delle reti e dell'informazione
BCE	Banca centrale europea	EPO	Ordine di protezione europeo
BEI	Banca europea per gli investimenti	EPSO	Ufficio europeo di selezione del personale
CdC	Corte dei conti	ERCEA	Agenzia esecutiva del Consiglio europeo della ricerca
CdR	Comitato delle regioni	EWRS	Sistema di allarme rapido e di reazione
CE	Comunità europee	FRA	Agenzia dell'Unione europea per i diritti fondamentali
CGAM	Comitato di gestione dell'assicurazione comune contro le malattie	GLA29	Gruppo di lavoro Articolo 29 per la protezione dei dati
CGE	Corte di giustizia europea	GLPG	Gruppo di lavoro Polizia e giustizia
CPAS	<i>Comité de Préparation pour les Affaires Sociales</i>	HR	Risorse umane
CPD	Coordinatore della protezione dei dati	IAS	Servizio di audit interno
DDA	Dichiarazione di affidabilità	IMI	Sistema d'informazione del mercato interno
DG INFSO	Direzione generale Società dell'informazione e mezzi di comunicazione	IOM	Organizzazione internazionale per le migrazioni
DG MARKT	Direzione generale Mercato interno e servizi	ISS	Strategia di sicurezza interna
DIGIT	Direzione generale Informatica	JRC	Centro comune di ricerca
EAS	Scuola europea di amministrazione	JRO	Operazione di rimpatrio congiunto
EASA	Agenzia europea per la sicurezza aerea	JSB	Organo comune di controllo
ECDC	Centro europeo per la prevenzione e il controllo delle malattie	LIBE	Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo
ECHR	Convenzione europea dei diritti dell'uomo	LISO	Responsabile locale della sicurezza delle informazioni
EEA	Agenzia europea dell'ambiente	LSO	Responsabile locale della sicurezza
EFSA	Autorità europea per la sicurezza alimentare	OLAF	Ufficio europeo per la lotta antifrode
EIO	Ordine europeo di indagine penale	PNR	Codice di prenotazione/Scheda nominativa del passeggero

R&S	Ricerca e sviluppo
RFID	Identificazione a radiofrequenza
RPD	Responsabile della protezione dei dati
SID	Sistema d'informazione doganale
SIS	Sistema d'informazione Schengen
SIV	Sistema d'informazione visti
SOC	Centro operativo dei servizi
s-TESTA	Servizi transeuropei per la comunicazione telematica tra amministrazioni
SWIFT	Società per le telecomunicazioni finanziarie interbancarie mondiali
TFTP	Programma di controllo delle transazioni finanziarie dei terroristi
TFUE	Trattato sul funzionamento dell'Unione europea
TI	Tecnologia dell'informazione
TIC	Tecnologie dell'informazione e della comunicazione
TURBINE	TrUsted Revocable Biometrics IdeNtitiEs
UAMI	Ufficio per l'armonizzazione nel mercato interno
UE	Unione europea
UNHCR	Alto Commissariato delle Nazioni Unite per rifugiati
WCO	Organizzazione mondiale delle dogane

Allegato D — Elenco dei responsabili della protezione dei dati

ORGANIZZAZIONE	NOME	E-MAIL
Parlamento europeo (PE)	Jonathan STEELE	Data-Protection@europarl.europa.eu
Consiglio europeo (Consilium)	Pierre VERNHES	Data.Protection@consilium.europa.eu
Commissione europea (CE)	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Corte di giustizia delle Comunità europee (CURIA)	Marc SCHAUSS	Dataprotectionofficer@curia.europa.eu
Corte dei conti europea (CdC)	Johan VAN DAMME	Data-Protection@eca.europa.eu
Comitato economico e sociale europeo (CESE)	Maria ARSENE	Data.Protection@eesc.europa.eu
Comitato delle regioni (CdR)	Rastislav SPÁC	Data.Protection@cor.europa.eu
Banca europea per gli investimenti (BEI)	Jean-Philippe MINNAERT	Dataprotectionofficer@eib.org
Mediatore europeo	Loïc JULIEN	DPO-euro-ombudsman@ombudsman.europa.eu
Garante europeo della protezione dei dati (GEPD)	Alfonso SCIROCCO, Sylvie PICARD (Assistant DPO)	alfonso.scirocco@edps.europa.eu
Banca centrale europea (BCE)	Frederik MALFRÈRE	DPO@ecb.int
Ufficio europeo per la lotta antifrode (OLAF)	Laraine LAUDATI	Laraine.Laudati@ec.europa.eu
Centro di traduzione degli organismi dell'Unione europea (CDT)	Benoît VITALE	Data-Protection@cdt.europa.eu
Ufficio per l'armonizzazione nel mercato interno (UAMI)	Ignacio DE MEDRANO CABALLERO	DataProtectionOfficer@oami.europa.eu
Agenzia europea per i diritti fondamentali (FRA)	Nikolaos FIKATAS	Nikolaos.Fikatas@fra.europa.eu
Agenzia europea per i medicinali (EMA)	Vincenzo SALVATORE	Data.Protection@emea.europa.eu
Ufficio comunitario delle varietà vegetali (UCVV)	Véronique DOREAU	Doreau@cpvo.europa.eu
Fondazione europea per la formazione professionale (ETF)	Liia KAARLOP	Liia.Kaarlop@etf.europa.eu
Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)	Emmanuel MAURAGE	Dataprotection@enisa.europa.eu
Fondazione europea per il miglioramento delle condizioni di vita e di lavoro (Eurofound)	Markus GRIMMEISEN	MGR@eurofound.europa.eu
Osservatorio europeo delle droghe e delle tossicodipendenze (OEDT)	Cecile MARTEL	Cecile.Martel@emcdda.europa.eu

>>>

ORGANIZZAZIONE	NOME	E-MAIL
Autorità europea per la sicurezza alimentare (EFSA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu
Agenzia europea per la sicurezza marittima (EMSA)	Małgorzata NESTEROWICZ	Malgorzata.Nesterowicz@emsa.europa.eu
Centro europeo per lo sviluppo della formazione professionale (Cedefop)	Spyros ANTONIOU	Spyros.Antoniou@cedefop.europa.eu
Agenzia esecutiva per l'istruzione, gli audiovisivi e la cultura (EACEA)	Hubert MONET	eacea-data-protection@ec.europa.eu
Agenzia europea per la sicurezza e la salute sul lavoro (OSHA)	Terry TAYLOR	Taylor@osha.europa.eu
Agenzia comunitaria di controllo della pesca (CFCA)	Clara FERNANDEZ/Rieke ARNDT	cfca-dpo@cfca.europa.eu
Autorità europea di vigilanza GNSS (GSA)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
Agenzia ferroviaria europea (ERA)	Guido STÄRKLE (acting DPO)	Dataprotectionofficer@era.europa.eu
Agenzia esecutiva per la salute e i consumatori (EAHC)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
Centro europeo per la prevenzione e il controllo delle malattie (ECDC)	Elisabeth ROBINO	Elisabeth.Robino@ecdc.europa.eu
Agenzia europea dell'ambiente (EEA)	Gordon McINNES	Gordon.McInnes@eea.europa.eu
Fondo europeo per gli investimenti (FEI)	Jobst NEUSS	J.Neuss@eif.org
Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne degli Stati membri dell'Unione europea (Frontex)	Sakari VUORENSOLA	Sakari.Vuorensola@frontex.europa.eu
Agenzia europea per la sicurezza aerea (EASA)	Francesca PAVESI	Francesca.Pavesi@easa.europa.eu
Agenzia esecutiva per la competitività e l'innovazione (EACI)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu
Agenzia esecutiva per la rete transeuropea di trasporto (TEN-T EA)	Zsófia SZILVÁSSY	Zsofia.Szilvassy@ec.europa.eu
Agenzia europea per i prodotti chimici (ECHA)	Alain LEFÈBVRE	Minna.Heikkila@echa.europa.eu
Agenzia esecutiva del Consiglio europeo della ricerca (ERCEA)	Donatella PIATTO	Donatella.Piatto@ec.europa.eu
Agenzia esecutiva per la ricerca (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu

>>>

ORGANIZZAZIONE	NOME	E-MAIL
“Fusion for Energy” (Impresa comune europea per il progetto ITER e lo sviluppo dell’energia da fusione)	Radoslav HANAK	Radoslav.Hanak@f4e.europa.eu
Impresa comune SESAR (SESAR)	Daniella PAVKOVIC	Daniella.Pavkovic@sesarju.eu
Impresa comune Artemis	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Impresa comune Clean Sky	Silvia POLIDORI	Silvia.Polidori@cleansky.eu
Iniziativa sui farmaci innovativi (IMI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Impresa comune Celle a combustione e idrogeno	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu
Istituto europeo di innovazione e tecnologia (IET)	Camilo SOARES	Camilo.Soares@ext.ec.europa.eu

Allegato E — Elenco dei pareri su controlli preventivi

Analisi empirica delle correlazioni tra le variabili dei sistemi di lavoro e il processo decisionale - UAMI

Parere del 22 novembre 2010 su “Analisi empirica delle correlazioni tra le variabili dei sistemi di lavoro e il processo decisionale” riguardante una notifica dell’Ufficio per l’armonizzazione nel mercato interno (UAMI) del 22 luglio 2010 (fascicolo 2010-0468)

Procedure relative all’assunzione di agenti - BEI

Avviso di notifica dell’11 novembre 2010 su un controllo preventivo riguardante le procedure di assunzione di agenti (fascicolo 2009-0254)

Procedura di assunzione e strumento elettronico di presentazione della domanda di assunzione - EASA

Lettera del 19 ottobre 2010 riguardante una notifica per controllo preventivo su “Procedura di assunzione dell’EASA e strumento elettronico di presentazione della domanda di assunzione”, (fascicolo 2010-0466)

Procedure relative alle indagini su casi di frode - BEI

Parere del 14 ottobre 2010 su una notifica per controllo preventivo riguardante le indagini su casi di frode nel gruppo BEI (fascicolo 2009-0459)

Distacco di esperti nazionali - CdR

Lettera del 5 ottobre 2010 su una notifica per controllo preventivo riguardante il distacco di esperti nazionali presso il Comitato delle regioni (fascicolo 2010-0515)

Trattamento di dati personali nel quadro delle detrazioni di stipendio in caso di sciopero - BCE

Parere del 28 settembre 2010 su una notifica per controllo preventivo riguardante il trattamento di dati personali nel quadro delle detrazioni di stipendio in caso di sciopero (fascicolo 2009-0514)

Selezione e assunzione di personale - EAHC

Lettera del 24 settembre 2010 su una notifica per controllo preventivo riguardante la selezione e assunzione di personale (agenti temporanei distaccati o non distaccati dalla Commissione europea, agenti a contratto, personale ad interim e apprendisti) presso l’Agenzia esecutiva per la salute e i consumatori (fascicolo 2010-0346)

Selezione di revisori esterni - Commissione (Ufficio delle pubblicazioni)

Parere del 6 settembre 2010 riguardante una notifica per controllo preventivo da parte del responsabile della protezione dei dati della Commissione europea su “Elenco dei partecipanti all’esame di revisori sotto contratto” (fascicolo 2010-400)

Ispezioni di sicurezza - Commissione (DG JRC Ispra)

Parere del 6 settembre 2010 riguardante una notifica per controllo preventivo da parte del responsabile della protezione dei dati della Commissione europea su “Ispezioni di sicurezza presso il Centro comune di ricerca di Ispra” (fascicolo 2009-682)

Sistema europeo di sorveglianza („TESSy”) - ECDC

Parere del 3 settembre 2010 su una notifica per controllo preventivo riguardante il sistema europeo di sorveglianza („TESSy”) del Centro europeo per la prevenzione e il controllo delle malattie (ECDC) (fascicolo 2009-0474)

Politica per la tutela della dignità della persona e la prevenzione di abusi psicologici e sessuali - EASA

Parere del 29 luglio 2010 riguardante una notifica per controllo preventivo su “Politica dell’EASA per la tutela della dignità della persona e la prevenzione di abusi psicologici e sessuali” (fascicolo 2010-318)

Applicazione della procedura informale nei casi di abusi psicologici e sessuali - CESE

Parere del 28 luglio 2010 riguardante una notifica per controllo preventivo su “Applicazione della procedura informale nei casi di abusi psicologici e sessuali nel Comitato” (fascicolo 2010-321)

Selezione e assunzione di agenti temporanei e a contratto, esperti nazionali distaccati e apprendisti - ECHA

Lettera del 27 luglio 2010 su una notifica per controllo preventivo riguardante la selezione e l'assunzione di agenti temporanei e a contratto, esperti nazionali distaccati e apprendisti (fascicolo 2010-0109)

Trattamento di dati personali nel contesto di un controllo della qualità del processo - Consiglio

Parere del 26 luglio 2010 su una notifica per controllo preventivo riguardante il trattamento di dati personali nel contesto di un controllo della qualità del processo (fascicolo 2009-0295)

Seguito amministrativo di assenze ingiustificate dovute a malattia - Consiglio

Parere del 22 luglio 2010 su una notifica per controllo preventivo riguardante il caso "Seguito amministrativo di assenze ingiustificate dovute a malattia" (fascicolo 2009-0687)

Procedura di giuramento di funzionari - OEDT

Lettera del 22 luglio 2010 su una notifica per controllo preventivo riguardante le attività di trattamento correlate alla procedura di giuramento per i funzionari dell'OEDT (fascicolo 2010-0407)

Procedure correlate alla "360° Leadership feedback report" - BEI

Parere del 20 luglio 2010 su una notifica per controllo preventivo riguardante le procedure correlate alla "360° Leadership feedback report" (fascicolo 2009-0215)

Procedura di promozione per funzionari e agenti - CESE

Parere del 19 luglio 2010 su "Procedura di promozione per funzionari e agenti" riguardante una notifica per controllo preventivo (fascicolo 2008-474)

Selezione e assunzione di personale temporaneo – Banca europea per gli investimenti - BEI

Lettera del 14 luglio 2010 su una notifica per controllo preventivo riguardante la selezione e l'assun-

zione di personale temporaneo (fascicolo 2009-0678)

Consultazione e aggiornamento della banca dati centrale sulle esclusioni – Comitato delle regioni

Parere del 4 giugno 2010 su una notifica per controllo preventivo riguardante il documento "Procedure per la consultazione e l'aggiornamento della banca dati centrale sulle esclusioni" (fascicolo 2010-248)

Procedura per la gestione di casi di incompetenza - Consiglio

Parere del 4 luglio 2010 su una notifica per controllo preventivo riguardante il documento "Procedura per la gestione di casi di incompetenza presso il segretariato generale del Consiglio" (fascicolo 2010-237)

Gestione e valutazione delle traduzioni esterne eseguite dalla DG TRAD - Parlamento

Parere del 4 giugno 2010 riguardante una notifica per controllo preventivo su "Gestione e valutazione delle traduzioni esterne eseguite dalla DG TRAD" (fascicolo 2009-0827)

Procedura di selezione di dipendenti temporanei - Commissione

Parere del 4 giugno 2010 su una notifica per controllo preventivo riguardante la procedura di selezione di dipendenti temporanei (fascicolo 2008-704)

Registrazione di un soggetto interessato nella banca dati centrale sulle esclusioni - Commissione

Parere del 26 maggio 2010 su una notifica per controllo preventivo riguardante l'operazione di trattamento di dati personali per la registrazione di un soggetto interessato nella banca dati centrale sulle esclusioni (fascicolo 2009-0681)

Procedura di nomina dei direttori generali, direttori e responsabili di unità – Parlamento europeo

Parere del 20 maggio 2010 su una notifica per controllo preventivo riguardante la procedura di nomina dei direttori generali, direttori e responsabili di unità (fascicolo 2010-0270)

Assunzione di END e tirocinanti – Centro europeo per la prevenzione e il controllo delle malattie (ECDC)

Lettera del 19 maggio 2010 su una notifica per controllo preventivo riguardante l'assunzione di END e tirocinanti (fascicolo 2009-0453)

Assunzione di agenti temporanei e a contratto – Agenzia europea dell'ambiente (EEA)

Lettera del 19 maggio 2010 su una notifica per controllo preventivo riguardante l'assunzione di agenti temporanei e a contratto (fascicolo 2009-0467)

Sostegno psico-sociale e finanziario – Centro comune di ricerca (JRC)

Parere del 10 maggio 2010 su una notifica per controllo preventivo riguardante il sostegno psico-sociale e finanziario al Centro comune di ricerca (JRC ITU) di Karlsruhe (fascicolo 2008-713)

Raccolta di nomi e taluni altri dati rilevanti dei rimpatriati nelle operazioni di rimpatrio congiunto- Frontex

Parere del 26 aprile 2010 riguardante una notifica per controllo preventivo su "Raccolta di nomi e taluni altri dati rilevanti dei rimpatriati nelle operazioni di rimpatrio congiunto (JRO)" (fascicolo 2009-0281)

Sistema di allarme rapido e di reazione (EWRS)– Commissione europea

Parere del 26 aprile 2010 su una notifica per controllo preventivo riguardante il sistema di allarme rapido e di reazione (EWRS) (fascicolo 2009-0137)

Promozione interna di funzionari e riclassificazione di agenti temporanei - OEDT

Parere del 22 aprile 2010 su una notifica per controllo preventivo riguardante la promozione interna di funzionari e la riclassificazione di agenti temporanei (fascicolo 2009-0839)

Operazioni di trattamento per la gestione delle gare d'appalto - ETF

Parere del 22 aprile 2010 su una notifica per controllo preventivo riguardante le operazioni di trattamento per la gestione delle gare d'appalto (fascicolo 2009-0037)

Incompetenza professionale – Corte di giustizia europea

Parere del 21 aprile 2010 su una notifica per controllo preventivo riguardante la procedura di gestione dei casi di incompetenza professionale (fascicolo 2009-860)

Indagini amministrative e procedure disciplinari - EMA

Parere del 21 aprile 2010 su una notifica per controllo preventivo riguardante il trattamento di dati personali nelle indagini amministrative e nelle procedure disciplinari (fascicolo 2010-0047)

Procedure di appalto e inviti a presentare manifestazione di interesse per la selezione di esperti - Commissione

Parere del 15 aprile 2010 riguardante una notifica per controllo preventivo su "Procedure di appalto e inviti a presentare manifestazione di interesse per la selezione di esperti" (fascicolo 2009-570)

Leadership Effectiveness - Commissione

Parere del 7 aprile 2010 riguardante una notifica per controllo preventivo su "Leadership Effectiveness" (fascicolo 2010-0002)

Procedure di selezione del personale tramite commissioni - BEI

Parere del 26 marzo 2010 riguardante una notifica per controllo preventivo su "procédures relatives à la sélection du personnel par des panels" (fascicolo 2009-679)

Gestione dei periodi di ferie - Parlamento

Parere del 25 marzo 2010 su una notifica per controllo preventivo riguardante la gestione dei periodi di ferie (fascicolo 2009-595)

Compilazione manuale di documenti di visitatori concernenti disabilità – Parlamento europeo

Parere del 16 marzo 2010 riguardante una notifica per controllo preventivo su "Compilazione manuale di documenti di visitatori concernenti disabilità" (fascicolo 2009-564)

Procedura di mobilità interna - UAMI

Parere del 15 marzo 2010 su una notifica per controllo preventivo da parte del responsabile della protezione dei dati dell'Ufficio per l'armonizzazione nel mercato interno riguardante la mobilità interna (fascicolo 2008-426)

Scuola europea di amministrazione - BELBIN Self perception inventory - Commissione europea

Parere del 15 marzo 2010 riguardante una notifica per controllo preventivo da parte del responsabile della protezione dei dati della Commissione europea su "Scuola europea di amministrazione - BELBIN Self perception inventory" (fascicolo 2009-377)

Valutazione della prestazione - OEDT

Parere ripreso in una lettera dell'8 marzo 2010 su una notifica per controllo preventivo riguardante la valutazione della prestazione (fascicolo 2009-838)

Gestione delle assenze e dei congedi per malattia - CESE

Parere del 5 marzo 2010 su una notifica per controllo preventivo riguardante la gestione delle assenze e dei congedi per malattia mediante la banca dati Centurio (fascicoli congiunti 2009-0702 e 2009-0703)

Selezione di consulenti di fiducia - FRA

Parere del 10 febbraio 2010 su una notifica per controllo preventivo riguardante le procedure di selezione per la selezione di consulenti di fiducia (fascicolo 2009-857)

Nomina di personale amministrativo di medio livello - Ufficio comunitario delle varietà vegetali (UCVV)

Parere del 28 gennaio 2010 su una notifica per controllo preventivo riguardante la nomina di personale amministrativo di medio livello (fascicolo 2009-0666)

e-Probation - Banca europea per gli investimenti

Parere del 21 gennaio 2010 su una notifica per controllo preventivo riguardante il trattamento di dati

personali nel quadro della gestione dei periodi di prova (e-probation) (fascicolo 2009-718)

Reclami dei membri - Comitato di gestione dell'assicurazione comune contro le malattie

Parere del 18 gennaio 2010 su una notifica per controllo preventivo da parte del Comitato di gestione dell'assicurazione comune contro le malattie riguardante il fascicolo "Reclami dei membri" (fascicolo 2009-070)

Accesso a unità e messaggi di posta elettronica privati - Corte dei conti

Parere del 18 gennaio 2010 riguardante una notifica per controllo preventivo su "Procedura per l'accesso a unità e messaggi di posta elettronica privati" (fascicolo 2009-620)

Allegato F — Elenco dei pareri su proposte legislative

Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

Parere del 20 dicembre 2010 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura

Parere del 17 dicembre 2010 sulla comunicazione della Commissione "La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura"

Eurodac

Parere del 15 dicembre 2010 sull'istituzione dell'EURODAC per il confronto delle impronte digitali

Proposta di regolamento relativo all'immissione sul mercato e all'uso di precursori di esplosivi

Parere del 15 dicembre 2010 sulla proposta di regolamento relativo all'immissione sul mercato e all'uso di precursori di esplosivi

La politica antiterrorismo dell'UE: principali risultati e sfide future

Parere del 24 novembre 2010 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio "La politica antiterrorismo dell'UE: principali risultati e sfide future"

Approccio globale al trasferimento dei dati del codice di prenotazione verso paesi terzi

Parere del 19 ottobre 2010 sull'approccio globale al trasferimento dei dati del codice di prenotazione (PNR) verso paesi terzi

Ordine europeo di protezione e ordine europeo di indagine penale

Parere del 5 ottobre 2010 sull'ordine di protezione europeo e sull'ordine europeo di indagine penale

Gestione delle informazioni nello spazio di libertà, sicurezza e giustizia

Parere del 30 settembre 2010 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio "Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia"

Sistemi di garanzia dei depositi

Parere del 9 settembre 2010 sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa ai sistemi di garanzia dei depositi (rifusa)

Trattamento e trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP II)

Parere del 22 giugno 2010 sulla proposta di decisione del Consiglio sulla conclusione di un accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP II)

Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne degli Stati membri dell'Unione europea (FRONTEX)

Parere del 17 maggio 2010 sulla proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento del Consiglio (CE) n. 2007/2004 che istituisce un'Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne degli Stati membri dell'Unione europea (Frontex)

Abuso sessuale di minori e pedopornografia

Parere del 10 maggio 2010 sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pedopornografia, che abroga la decisione quadro 2004/68/GAI

Iniziativa dei cittadini

Parere del 21 aprile 2010 sulla proposta di regolamento del Parlamento europeo e del Consiglio riguardante l'iniziativa dei cittadini

Rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

Parere del 14 aprile 2010 sulla proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

Promozione della fiducia nella società dell'informazione

Parere del 18 marzo 2010 sulla promozione della fiducia nella società dell'informazione tramite l'incentivazione della protezione dei dati e della vita privata

Comitato misto di cooperazione doganale UE-Giappone

Parere del 12 marzo 2010 sulla proposta di decisione del Consiglio relativa alla posizione dell'Unione in seno al Comitato misto di cooperazione doganale UE-Giappone in materia di riconoscimento reciproco dei programmi di operatore economico autorizzato nell'Unione europea e in Giappone

Accordo commerciale anticontraffazione (ACTA)

Parere del 22 febbraio 2010 in merito ai negoziati attualmente condotti dall'Unione europea per il raggiungimento di un accordo commerciale anticontraffazione (ACTA)

Incidenti e inconvenienti nel settore dell'aviazione civile

Parere del 4 febbraio 2010 sulla proposta di regolamento del Parlamento europeo e del Consiglio in materia di inchieste e prevenzione di incidenti e inconvenienti nel settore dell'aviazione civile

Cooperazione nel settore fiscale

Parere del 6 gennaio 2010 sulla proposta di direttiva del Consiglio relativa alla cooperazione amministrativa nel settore fiscale

Allegato G — Discorsi del Garante e del Garante aggiunto

Il Garante e il Garante aggiunto hanno continuato a dedicare sforzi e tempo considerevoli per illustrare la loro missione e sensibilizzare l'opinione pubblica sulla tematica della protezione dei dati in generale nonché su una serie di questioni specifiche mediante discorsi e contributi analoghi presso varie istituzioni e in diversi Stati membri nel corso dell'anno.

Parlamento europeo – Commissioni

27 gennaio	Garante aggiunto, commissione LIBE sulle politiche antiterrorismo (Bruxelles) (*)
4 marzo	Garante, commissione LIBE su PNR e tutela della vita privata nelle relazioni transatlantiche (Bruxelles)
21 giugno	Garante, commissione LIBE sulla Carta dei diritti fondamentali (Bruxelles) (*)
23 giugno	Garante, commissione LIBE sull'accordo TFTP II (Bruxelles)
28 settembre	Garante aggiunto, comm. LIBE sulla lotta contro l'abuso sessuale (Bruxelles) (*)
9 novembre	Garante, commissione PETI sull'accesso del pubblico ai documenti (Bruxelles) (*)
15 novembre	Garante e Garante agg., comm. LIBE sulla relazione annuale 2009 (Bruxelles)

Parlamento europeo – altri

28 gennaio	Garante, Giornata della protezione dei dati (Bruxelles)
9 febbraio	Garante, Giornata per un'Internet più sicura (Strasburgo) (*)
16 marzo	Garante, Gli eurodeputati e l'ACTA (Bruxelles)

24 marzo	Garante aggiunto, Piattaforma per la tutela della vita privata: libertà in Internet (Bruxelles)
8 aprile	Garante, Gli eurodeputati e il PNR (Bruxelles)
1° dicembre	Garante, Piattaforma per la tutela della vita privata: Revisione della protezione dei dati (Bruxelles)

Consiglio

19 gennaio	Garante aggiunto, Conferenza su ECRIS (Bruxelles) (*)
25 gennaio	Garante, Rappresentanza polacca, Giornata della protezione dei dati (Bruxelles)
11 febbraio	Garante, Conferenza su Fiducia nelle TIC (Leon) (*)
24 marzo	Garante, Gruppo di lavoro sulla protezione dei dati (Bruxelles)

Commissione

28 gennaio	Garante, Giornata della protezione dei dati, mini-simposio (Bruxelles)
28 gennaio	Garante, Giornata della protezione dei dati, discorso a pranzo ufficiale (Bruxelles)
22 giugno	Garante, Conferenza sui sistemi di trasporto intelligenti (Bruxelles) (*)
29 giugno	Garante e Garante aggiunto, Audizione sulla revisione della protezione dei dati (Bruxelles)
22 settembre	Garante, Task force per i servizi delle reti sociali (Bruxelles)
5 ottobre	Garante, Tavola rotonda sul futuro della protezione dei dati pers. (Bruxelles) (*)
18 novembre	Garante, Conferenza OLAF (Parigi) (*)
3 dicembre	Garante, Conferenza sulla direttiva relativa alla conserv. dei dati (Bruxelles) (*)

(*) Testo disponibile sul sito Internet del GEPD

Altre istituzioni e organismi comunitari

27 gennaio	Garante aggiunto, Giornata della protezione dei dati presso l'EMA (Londra-Bruxelles) (*)
7 maggio	Garante, Agenzia per i diritti fondamentali (Vienna)
27-28 maggio	Garante e Garante agg., Seminario sulle organizzazioni internazionali (Firenze)
31 maggio	Garante, Protezione dei dati e applicazione della legge (Treviri) (*)
7 giugno	Garante aggiunto, CESC sugli abusi cibernetici (Bratislava) (*)
15-16 giugno	Garante e Garante aggiunto, Protezione dei dati nella procedura penale (Madrid)
13 settembre	Garante, Scuola estiva ENISA-FORTH (Heraklion)
15 novembre	Garante e Garante aggiunto, Conferenza stampa sulla relazione annuale 2009 (Bruxelles) (*)

Conferenze internazionali

30 gennaio	Garante, Computer & protezione della vita privata e dei dati (Bruxelles)
10 marzo	Garante, Tavola rotonda su 30 anni di orientamenti OCSE per la tutela della vita privata (Parigi) (*)
20 aprile	Garante, Vertice IAPP sulla tutela globale della vita privata (Washington DC) (**)
29 aprile	Garante e Garante aggiunto, Autorità europee della protezione dei dati (Praga) (*)
6 luglio	Garante, Le leggi sulla tutela della vita privata e le imprese (Cambridge)
25 ottobre	Garante aggiunto, La voce pubblica della società civile (Gerusalemme) (*)

26 ottobre	Garante, 30 anni di orientamenti OCSE per la tutela della vita privata (Gerusalemme)
27 ottobre	Garante, Commissari per la protezione della vita privata e dei dati (Gerusalemme)
28 ottobre	Garante aggiunto, Commissari per la protezione della vita privata e dei dati (Gerusalemme) (*)

Altri eventi

22 gennaio	Garante aggiunto, 30° anniversario del CRID (Namur) (*)
2 febbraio	Garante, Congresso della polizia europea (Berlino) (*)
26 febbraio	Garante, Proprietà intellettuale e società dell'informazione (Barcellona) (*)
5 marzo	Garante, Colloquio PLN (Bruxelles)
9 marzo	Garante, Camera di commercio britannica in Belgio (Bruxelles) (*)
12 marzo	Garante aggiunto, Etica medica e diritti dei pazienti (San Remo)
23 marzo	Garante, Sessione parlamentare congiunta sulla sicurezza (Parigi) (*)
26 marzo	Garante, Mobilità globale e sicurezza (Bruxelles) (*)
13 aprile	Garante, Giornata europea per la promozione della sicurezza cibernetica (Bruxelles) (*)
23 aprile	Garante, Camera di commercio americana nell'UE (Bruxelles)
28 aprile	Garante aggiunto, Consiglio giudiziario (Roma)
11 maggio	Garante aggiunto, Seminario sul cloud computing (Bruxelles)

(*) Testo disponibile sul sito Internet del GEPD

(**) Video disponibile sul sito Internet del GEPD

20 maggio	Garante, Protezione dei dati intensiva (Londra)	29 settembre	Garante aggiunto, Sicurezza dei confini dell'UE (Bruxelles) (*)
1° giugno	Garante, Fiducia digitale (Bruxelles)	13 ottobre	Garante, Tutela della vita privata in un mondo digitale (Bruxelles)
2 giugno	Garante, L'Internet delle cose (Bruxelles)	22 ottobre	Garante aggiunto, Giustizia penale in Europa (Lussemburgo) (*)
8 giugno	Garante aggiunto, Tavola rotonda sulla sicurezza (Bruxelles)	5 novembre	Garante aggiunto, Conformità alla tutela della vita privata (Roma)
15 giugno	Garante aggiunto, Trattato di Lisbona (Londra)	17 novembre	Garante aggiunto, Trasporti intelligenti (Milano)
17 giugno	Garante aggiunto, Forum dei responsabili europei della tutela della vita privata (Bruxelles)	23 novembre	Garante, Tutela della vita privata e ricerca scientifica (Bruxelles) (*)
22 giugno	Garante, Camera di commercio americana nell'UE (Bruxelles)	23 novembre	Garante aggiunto, Ricerca medica e tutela della vita privata (Bruxelles) (*)
23 giugno	Garante, L'UE digitale e l'IAPP (Bruxelles)	24 novembre	Garante aggiunto, Seminario sulla protezione dei dati – videomessaggio (Buenos Aires)
29 giugno	Garante aggiunto, CEPS sui confini e sulla giustizia penale (Bruxelles)	29 novembre	Garante, Amici dell'Europa sulla protezione dei dati nell'UE (Bruxelles)
8 luglio	Garante aggiunto, Alma Graduate School (Bologna)	30 novembre	Garante, Forum Europa sulla protezione dei dati nell'UE (Bruxelles)
12 luglio	Garante aggiunto, Consiglio giudiziario (Roma)	30 novembre	Garante, Forum europeo su Internet (Bruxelles)
7 settembre	Garante, Sicurezza futura (Berlino)	2 dicembre	Garante, Hogan & Lovells (Londra)
15 settembre	Garante, Tutela della vita privata e sicurezza (Bruxelles)	9 dicembre	Garante, Etica e governance della biometria (Bruxelles) (*)
16 settembre	Garante, Consiglio di Lisbona sul mercato digitale (Bruxelles)	10 dicembre	Garante aggiunto, Diritti dei passeggeri comunitari (Treviri)
20 settembre	Garante, Antiterrorismo e protezione dei dati (Bruxelles)	16 dicembre	Garante, Assemblea sull'Internet del futuro (Gand) (*)
23 settembre	Garante, Seminario sulla revisione della protezione dei dati (Bruxelles)		
28 settembre	Garante, Protezione dei dati e libertà d'informazione (Budapest)		
29 settembre	Garante, Informazione, sicurezza e tutela della vita privata (Budapest)		

Allegato H — Organigramma del secretariato del GEPD



Il Garante e il Garante aggiunto con la maggior parte dei loro collaboratori.

• Controllo e applicazione della legge

Sophie LOUVEAUX <i>Capo del Settore Controllo e applicazione della legge</i>	John-Pierre LAMB <i>Esperto nazionale distaccato</i>
Laurent BESLAY <i>Coordinatore sicurezza e tecnologia</i>	Xanthi KAPSOSIDERI <i>Consigliere giuridico</i>
Jaroslaw LOTARSKI <i>Coordinatore reclami</i>	Luisa PALLA <i>Assistente per il controllo e l'applicazione della legge</i>
Maria Verónica PEREZ ASINARI <i>Coordinatore consulenza</i>	Dario ROSSI <i>Assistente per il controllo e l'applicazione della legge</i> <i>Corrispondente contabile</i> <i>Gestore dei depositi dati esterni (EDWM)</i>

Isabelle CHATELIER <i>Consigliere giuridico</i>	Tereza STRUNCOVA <i>Consigliere giuridico</i>
Bart DE SCHUITENEER <i>Consigliere responsabile per la tecnologia</i> <i>Responsabile locale della sicurezza/LISO</i>	Michaël VANFLETEREN <i>Consigliere giuridico</i>
Delphine HAROU <i>Consigliere giuridico</i>	

• **Politica e consulenza**

Hielke HIJMANS <i>Capo del Settore Politica e consulenza</i>	Raffaele DI GIOVANNI BEZZI <i>Assistente per la politica e la consulenza</i>
Bénédicte HAVELANGE <i>Coordinatore sistemi TI su larga scala e politica di frontiera</i>	Herke KRANENBORG <i>Consigliere giuridico</i>
Anne-Christine LACOSTE <i>Coordinatore della cooperazione con le autorità di protezione dei dati</i>	Roberto LATTANZI <i>Esperto nazionale distaccato</i>
Rosa BARCELO <i>Consigliere giuridico</i>	Alfonso SCIROCCO <i>Responsabile della protezione dei dati</i> <i>Gestione della qualità</i>
Zsuzsanna BELENYESSY <i>Consigliere giuridico</i>	Luis VELASCO <i>Consigliere per la tecnologia</i>
Katarzyna CUADRAT-GRZYBOWSKA <i>Consigliere giuridico</i>	

• **Registrazione e supporto operativo**

Andrea BEACH <i>Capo del Settore Registrazione e supporto operativo</i>	Kim Thien LÊ <i>Assistente amministrativo</i>
Christine HUC <i>Assistente amministrativo</i>	Ewa THOMSON <i>Assistente amministrativo</i>
Kim DAUPHIN <i>Assistente amministrativo</i>	

• Informazione e comunicazione

Nathalie VANDELLE <i>Capo del Settore Informazione e comunicazione</i>	Agnieszka NYKA <i>Assistente per l'informazione e la comunicazione</i>
Olivier ROSSIGNOL <i>Assistente per l'informazione e la comunicazione</i>	

• Risorse umane, bilancio e amministrazione

Leonardo CERVERA NAVAS <i>Capo del Settore Risorse umane, bilancio e amministrazione</i>	Aida PASCU <i>Assistente amministrativo</i> <i>Assistente responsabile locale della sicurezza</i>
Isabelle DELATTRE <i>Assistente finanziario e contabile</i>	Sylvie PICARD <i>Assistente responsabile della protezione dei dati</i> <i>COFO - ICO</i>
Anne LEVÊCQUE <i>Assistente per le risorse umane</i> <i>GECO</i>	Anne-Françoise REYNDERS <i>Assistente amministrativo</i>
Vittorio MASTROJENI <i>Consigliere per le risorse umane</i>	Marian SANCHEZ LOPEZ <i>Consigliere finanziario e contabile</i>

Garante europeo della protezione dei dati

Relazione annuale 2010

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea

2011 — 118 pagg. — 21 x 29,7 cm

ISBN 978-92-95073-22-7

doi:10.2804/21740

Come ottenere le pubblicazioni dell'Unione europea

Pubblicazioni gratuite:

- tramite EU Bookshop (<http://bookshop.europa.eu>);
- presso le rappresentanze o le delegazioni dell'Unione europea.
Per ottenere indicazioni e prendere contatto collegarsi a <http://ec.europa.eu>
o inviare un fax al numero +352 2929-42758.

Pubblicazioni a pagamento:

- tramite EU Bookshop (<http://bookshop.europa.eu>).

Abbonamenti a pagamento (ad esempio serie annuali della *Gazzetta ufficiale dell'Unione europea*, raccolte della giurisprudenza della Corte di giustizia):

- tramite gli uffici vendita dell'Ufficio delle pubblicazioni dell'Unione europea (http://publications.europa.eu/others/agents/index_it.htm).



GARANTE EUROPEO
DELLA PROTEZIONE DEI DATI

*Garante europeo della
protezione dei dati*

www.edps.europa.eu



■ Ufficio delle pubblicazioni

ISBN 978-92-95073-22-7



9 789295 073227