



Una sintesi di questo rapporto, che offre una panoramica dei principali sviluppi nelle attività del GEPD nel 2018, è inoltre disponibile.

Ulteriori dettagli sulle GEPD possono essere trovate sul nostro sito web <http://www.edps.europa.eu> .

Il sito descrive inoltre un [sottoscrizione](#) caratteristica alla nostra newsletter.

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2019

© Foto: iStockphoto / GEPD e Unione Europea

© europeo della protezione dei dati 2019

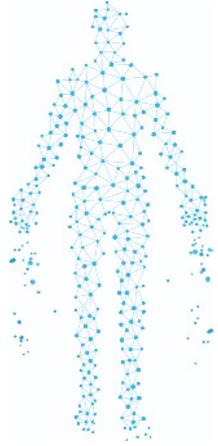
Riproduzione autorizzata con citazione della fonte.

Per qualsiasi uso o riproduzione di foto o altro materiale che non è sotto il copyright garante europeo della protezione dei dati,

l'autorizzazione deve essere richiesta direttamente dal detentori del copyright PDF

	ISBN 978-92-9242-280-6	ISSN 1830-9585 doi: 10,2804 / 801.791 QT-AA-19-001-IT-N	
Stampare	ISBN 978-92-9242-282-0	ISSN 1830-5474 doi: 10,2804 / 17012	QT-AA-19-001-IT-C
HTML	ISBN 978-92-9242-281-3	ISSN 1830-9585 doi: 10,2804 / 793.717	QT-AA-19-001-IT-Q

**P** Stampato su elementare -Cloro carta sbiancata ( ECF)



ANNUAL  
**REPORT**

---

2 0 1 8

Protezione dei dati europea

---

# CONTENUTI

▶	<b>PREFAZIONE</b>	<b>5</b>
▶	<b>MISSIONE, VALORI E PRINCIPI</b>	<b>7</b>
▶	<b>GEPD STRATEGIA 2015-2019</b>	<b>8</b>
	<b>1. Circa il GEPD</b>	<b>9</b>
	<b>1.1 Supervisione e l'esecuzione</b>	<b>9</b>
	<b>1.2 Politica e consultazione</b>	<b>10</b>
	<b>1.3 Monitoraggio sviluppi tecnologici</b>	<b>10</b>
	<b>2. 2018 - Una panoramica</b>	<b>11</b>
	<b>2.1 Nuova normativa per una nuova era</b>	<b>11</b>
	<b>2.2 Trovare un equilibrio tra sicurezza e privacy</b>	<b>12</b>
	<b>2.3 lo sviluppo di partnership</b>	<b>12</b>
	<b>2.4 Etica Digitale e la conferenza internazionale</b>	<b>13</b>
	<b>2.5 amministrazione interna</b>	<b>13</b>
	<b>2.6 Comunicare la protezione dei dati</b>	<b>13</b>
	<b>2.7 Key Performance Indicators 2018</b>	<b>14</b>
	<b>3. Obiettivi principali per il 2019</b>	<b>16</b>
	<b>4. 2018 Sintesi</b>	<b>19</b>
	<b>4.1 Preparazione per un nuovo quadro legislativo</b>	<b>19</b>
	4.1.1 L'EDPB si mette al lavoro	20
	4.1.2 Il regolamento protezione dei dati per le istituzioni dell'UE	21
	4.1.3-privacy: il completamento del quadro di protezione dei dati dell'UE	22
	4.1.4 Privacy by Design: la tecnologia che serve il popolo	25
	<b>4.2 supervisione Europol</b>	<b>25</b>
	4.2.1 cooperazione continua con l'unità di protezione dei dati dell'Europol	25
	4.2.2 Supervisione progetti analisi operativa	26
	4.2.3 Ispezione Europol	26
	4.2.4 Consulenza Europol	27
	4.2.5 vengono trattati i reclami	28
	4.2.6 Incontro con il Consiglio di cooperazione	28
	4.2.7 Impostazione del tono a livello di gestione	29
	4.2.8 Il Joint esame parlamentare Gruppo	29
	<b>4.3 Sicurezza e confini dell'UE</b>	<b>30</b>
	4.3.1 Il controllo efficace dei sistemi IT su larga scala	30
	4.3.2 controllo coordinato di sistemi IT su larga scala	31

4.3.3	Observing Schengen	31
4.3.4	Tutela dei diritti fondamentali nel settore della libertà, sicurezza e giustizia	32
<b>4.4.</b>	<b>Per terra</b>	<b>34</b>
4.4.1	La funzione DPO: istituzioni dell'UE guidare con l'esempio	35
4.4.2	Rafforzare la responsabilità delle istituzioni UE	36
4.4.3	Responsabilità in IT	36
4.4.4	dati notifiche di violazione: un how-to guida per le istituzioni dell'UE	37
4.4.5	La tutela della privacy nelle istituzioni dell'UE	37
4.4.6	Facendo con le istituzioni: verifiche e visite	43
4.4.7	controlli remoti di webservices	43
4.4.8	La trasparenza, il riutilizzo e la protezione dei dati	44
4.4.9	indagini transfrontaliere di natura diversa	44
4.4.10	domanda per il ritorno	45
4.4.11	verifiche di sicurezza di appaltatori esterni	45
4.4.12	Supervisione l'Autorità di vigilanza EFTA	45
4.4.13	Eurojust: un nuovo ruolo di vigilanza per il GEPD	46
4.4.14	Consulenza alle istituzioni dell'UE	46
4.4.15	Nuove tecnologie	48
4.4.16	Privacy ingegneria guadagnando terreno	48
4.4.17	manipolazione online e dei dati personali	49
4.4.18	Un approccio più coerente alle sfide nel ecosistema digitale: la stanza di compensazione Digital 50	
<b>4.5.</b>	<b>Affari internazionali</b>	<b>50</b>
4.5.1	trasferimenti internazionali di dati	51
4.5.2	Cooperazione internazionale	51
<b>4.6</b>	<b>Etica digitale</b>	<b>53</b>
4.6.1	Il gruppo consultivo etico: Segnalazione di etica Digital	54
4.6.2	Ottenere le vostre opinioni su Etica Digitale	54
4.6.3	incoraggiando il dibattito in tutto il mondo	55
<b>4.7</b>	<b>La Conferenza internazionale di protezione dei dati e della privacy 2018</b>	<b>56</b>
4.7.1	Il Closed Session - Etica e Intelligenza Artificiale	56
4.7.2	Il Sessione pubblica - Debating Etica	57
4.7.3	Eventi collaterali	59
4.7.4	Eventi sociali	59
Comunicazione 4.7.5	Conference	60
<b>5.</b>	<b>Casi Court</b>	<b>62</b>
<b>6.</b>	<b>Trasparenza e accesso ai documenti</b>	<b>63</b>
<b>7.</b>	<b>Il Segretariato</b>	<b>64</b>
<b>7.1</b>	<b>Informazione e comunicazione</b>	<b>64</b>
7.1.1	dei media online	64
7.1.2	Eventi e pubblicazioni	65
7.1.3	Relazioni esterne	67
7.1.4	L'EDPB	68
<b>7.2</b>	<b>Amministrazione, bilancio e personale</b>	<b>68</b>
7.2.1	Bilancio e finanze	68
7.2.2	Preparazione per la segreteria EDPB	69
7.2.3	Un concorso per gli specialisti della protezione dei dati	70
7.2.4	Il GDPR per EUI: preparazioni HR	70
7.2.5	Migliorare le politiche HR	70

8. La protezione dei dati Officer presso il GEPD	72
8.1 Il DPO presso il GEPD	72
8.2 Il passaggio a un nuovo regolamento	72
8.3 Consulenza l'istituzione e il miglioramento del livello di protezione	73
8.4 Richieste e lamentele	73
8.5 La sensibilizzazione all'interno del GEPD	73
8.6 La collaborazione con gli RPD nelle altre istituzioni dell'UE	73

Allegato A - Quadro giuridico	74
-------------------------------	----

Allegato B - Estratto dal regolamento (UE) 2018/1725	77
--	----

Allegato C - Elenco dei responsabili della protezione dei dati	80
--	----

Allegato D - Elenco dei controllo preventivo e le opinioni di controllo non-precedenti	82
--	----

Allegato E - Lista dei pareri e commenti formali sulle proposte legislative	85
---	----

Allegato F - Discorsi dal supervisore e garante nel 2018	86
--	----

Allegato G - Composizione del GEPD Segreteria	90
---	----

## **Tabelle e grafici**

Figura 1. tabella di analisi GEPD KPI	15
Figura 2. programma di formazione GEPD 2018	23
Figura 3. Evoluzione del numero di denunce, tra cui denunce irricevibili, ricevuto dal GEPD	39
Figura 4. istituzioni e gli organi interessati da denunce ricevute dal GEPD UE	39
Figura 5. Tipo di violazione presunta dei reclami ricevuti da GEPD	40
Figura 6. Evoluzione delle notifiche ricevute dalla GEPD	41
Figura 7. Evoluzione delle opinioni controlla preliminari rilasciate da GEPD	41
Figura 8. Percentuale scissione tra core business e le attività di amministrazione Nelle comunicazioni ricevute dal GEPD	42



## | Prefazione

2018 hanno dimostrato la potenza e le limitazioni della protezione dei dati.

Due anni dopo la sua adozione, il 25 maggio 2018 il regolamento sulla protezione dei dati generali (GDPR) è diventato pienamente applicabile.

Le persone hanno notato perché sono stati bombardati con messaggi di posta elettronica identikit, ogni informandoli di una politica di privacy aggiornata e, nella maggior parte dei casi, chiedendo che lo accettano di continuare a utilizzare il servizio. Finora, invece di adattare il loro modo di lavorare per proteggere meglio gli interessi di coloro che utilizzano i loro servizi, le aziende sembrano essere il trattamento della GDPR più come un puzzle legale, al fine di preservare il proprio modo di fare le cose.

Dovremmo aspettarci questo per cambiare il prossimo anno, tuttavia.

La più grande minaccia per la libertà e la dignità individuale deriva dalla eccessiva potere informativo di alcune aziende, o regolatori, e il più ampio, ecosistema incompressibile di inseguitori, profiler e targeters che sono in grado di raccogliere e utilizzare queste informazioni.

Appena tre mesi prima della GDPR diventato pienamente esecutive, l'abuso dei dati personali è diventato Headline News e oggetto di inchieste ufficiali, non solo nel Parlamento europeo, ma anche nelle capitali nazionali, da Washington DC a Londra a Delhi. I politici pubblici sono ora molto vivo alla minaccia la situazione attuale pone, non solo per la libertà dei consumatori nell'ambiente eCommerce, ma anche per la stessa democrazia.

L'intero sistema è suscettibile, non solo per le violazioni, ma anche alla manipolazione da parte di attori con agende politiche che mirano a minare la fiducia e la coesione sociale. La cartina di tornasole di come robusto regime giuridico della UE è in realtà sarà l'integrità delle elezioni del Parlamento europeo nel 2019.

l'applicazione coerente di tutte le regole, compresa la protezione dei dati, per prevenire e punire interferenza illecita durante le elezioni, sarà di vitale importanza. Abbiamo quindi Deploriamo profondamente il ritardo nell'adozione di regole aggiornate sulla e-privacy. Senza queste regole aggiornate per garantire il rispetto del, le informazioni sensibili più intimo e di comunicazione privati, aziende e privati rimangono esposti e vulnerabili, soggetti a un mosaico di leggi comunitarie e incertezza del diritto che non riescono a fornirci il controllo su noi stessi digitali.

Tuttavia, il programma di riforme di protezione dei dati nell'UE ha segnato una vittoria importante prima della fine dell'anno. In data 11 dicembre 2018, l'entrata in vigore di una GDPR per le istituzioni dell'UE ha assicurato che tutte 66 le istituzioni dell'UE e gli organi che supervisionano, così come il GEPD stesso, sono ora soggetti allo stesso rigore come controllori sotto la GDPR.

Dopo due anni di intensa preparazione, durante il quale abbiamo lavorato in stretta collaborazione non solo con le nostre controparti di protezione dei dati nelle istituzioni, ma anche con il top management e gli altri dipendenti europei, le istituzioni dell'UE sono ora in grado di dare l'esempio nella loro attuazione le norme sulla protezione dei dati.

Alla Conferenza internazionale di protezione dei dati e della privacy in ottobre, abbiamo avuto l'onore di mettere in mostra l'impegno dell'UE per l'etica e la dignità umana. autorità per la protezione dei dati del mondo ha aperto la strada nel controllo l'impatto umano di intelligenza artificiale, mentre una collezione straordinariamente ricca e diversificata di voci da tutto il mondo si sono riuniti in occasione della sessione pubblica della conferenza per discutere di come la tecnologia sta distruggendo la nostra vita e per chiamare per un nuovo consenso su ciò che è giusto e sbagliato nello spazio digitale. Noi continueremo a facilitare questa conversazione nel 2019 e oltre.

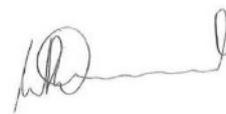
Su scala globale, la protezione dei dati continua a dimostrare la sua importanza geostrategica. Lo vediamo nel **dibattito in corso sulla Privacy Shield e l'imminente (ricambiato) decisione in merito alla adeguatezza delle** garanzie di protezione dei dati in Giappone. Vediamo anche che l'importanza data alla protezione dei dati nella comunità di applicazione della legge. Il nostro ruolo come un hands-on del regolatore dell'Agenzia europea di polizia, Europol, è ormai ben stabiliti, mentre alla fine del 2019 avremo assumere un ruolo simile per l'unità di cooperazione giudiziaria dell'Unione europea, Eurojust.

Il nuovo Consiglio europeo di protezione dei dati (EDPB), che ha iniziato i suoi lavori il 25 maggio 2018, si trova di fronte una sfida enorme per dimostrare che 29 autorità indipendenti possono agire come uno, nel rispetto gli uni degli altri approcci e metodi, ma convergenti verso un'applicazione riconoscibile e affidabile credibili europea cultura. Siamo lieti che la segreteria fornito dal GEPD era pienamente funzionante dal primo giorno del GDPR e continuerà a fornire assistenza dove siamo in grado di farlo.

Wojciech ed io sono ora nel l'ultimo anno del nostro mandato. Nel mese di marzo 2015, abbiamo pubblicato una raccomandazione in cui la nostra visione, obiettivi e punti di azione per gli anni a venire strategia. Nei prossimi mesi, pubblicheremo una recensione dei nostri sforzi in relazione alla strategia, assicurando che noi riteniamo responsabili per gli obiettivi che abbiamo fissato di nuovo nel 2015.



**Giovanni Buttarelli**  
Protezione dei dati europea



**Wojciech Wiewiórowski**  
Assistente supervisore

## Mission statement, values and principles

La protezione dei dati è un diritto fondamentale, protetto dalla legge europea e sancito dall'articolo 8 della [Carta dei diritti fondamentali dell'Unione europea](#).

Al fine di proteggere e garantire i diritti alla protezione dei dati e della privacy, il trattamento dei dati personali è soggetto al controllo di un'autorità indipendente. Il garante europeo della protezione dei dati (GEPD) è l'autorità di protezione dei dati indipendente dell'Unione europea, con il compito di garantire che le istituzioni e gli organi dell'UE rispettino il diritto alla protezione dei dati.

In accordo con [regolamento 2018/1725](#), e con [regolamento 45/2001](#) in precedenza, l'UE nel suo processo decisionale, legiferare e l'entità giudiziaria guarda al GEPD in quanto supervisore indipendente e imparziale, consulente sulle politiche e proposte di legge che potrebbero incidere sui diritti alla privacy e alla protezione dei dati. Il GEPD esegue queste funzioni stabilendosi come centro di eccellenza nella legge, e anche in tecnologia, in quanto riguarda o è influenzato dal trattamento dei dati personali.

Svolgiamo le nostre funzioni in stretta cooperazione con le autorità compagne di protezione dei dati come parte del Comitato europeo per la protezione dei dati (EDPB), e puntiamo ad essere il più trasparente possibile nel nostro lavoro di interesse pubblico nell'UE. Sotto il [regolamento generale sulla protezione dei dati](#), il GEPD è anche responsabile di fornire la segreteria al EDPB.

Il nostro approccio ai nostri compiti e il modo in cui lavoriamo con i nostri stakeholder sono guidati dai seguenti valori e principi:

### valori fondamentali

- **Imparzialità** - lavoro all'interno del quadro legislativo e politico dato a noi, essere indipendente e obiettiva, trovare il giusto equilibrio tra gli interessi in gioco.
- **Integrità** - sostenere i più alti standard di comportamento e di fare ciò che è giusto, anche se è impopolare.
- **Trasparenza** - spiegare quello che stiamo facendo e perché, in un linguaggio chiaro che è accessibile a tutti.
- **pragmatica** - comprendere le esigenze dei nostri stakeholder e la ricerca di soluzioni che funzionano nella pratica.

### Principi guida

- Serviamo l'interesse pubblico al fine di garantire che le istituzioni dell'UE rispettino i principi di protezione dei dati nella pratica. Contribuiamo alla politica di più ampio per quanto essa riguarda la protezione dei dati europea.
- Utilizzando la nostra esperienza, autorità e poteri formali, ci proponiamo di costruire la consapevolezza della protezione dei dati come un diritto fondamentale e come una parte vitale di una buona politica pubblica e l'amministrazione per le istituzioni comunitarie.
- Concentriamo la nostra attenzione e gli sforzi su settori della politica o di amministrazione che presentano il più alto rischio di non conformità o il maggiore impatto sulla privacy. Agiamo selettivamente e proporzionalmente.

# GEPD STRATEGIA 2 015-2 019

Il **Strategia GEPD 2015-2019** è stata adottata il 2 marzo 2015, all'inizio del corrente mandato del GEPD. Definisce le nostre priorità e informa il nostro lavoro, fornendo una struttura attraverso cui promuovere una nuova cultura della protezione dei dati nelle istituzioni e negli organismi europei.

## A proposito della strategia

All'inizio del suo mandato nel 2015, il nuovo GEPD ha perfezionato una strategia per i prossimi cinque anni. Il suo obiettivo era quello di realizzare la sua visione di un'Unione europea che porta l'esempio nel dibattito sulla protezione dei dati e della privacy e di individuare soluzioni innovative in fretta.

Il piano strategico 2015-2019 riassume:

- le grandi sfide della protezione dei dati e privacy nel corso del mandato;
- tre obiettivi strategici e le dieci azioni di accompagnamento per rispondere a queste sfide;
- Come realizzare la strategia, attraverso una gestione efficace delle risorse, comunicazione chiara e valutazione della performance.

I nostri obiettivi e le ambizioni di costruire sui nostri punti di forza, i **successi e le lezioni apprese dal nostro attuazione strategia 2013-2014**: *Verso l'eccellenza nella protezione dei dati.*

## Visione, Obiettivi e Azione 2015-2019

La nostra visione è quella di aiutare l'UE dia l'esempio nel dialogo globale sulla protezione dei dati e della privacy nell'era digitale. Il nostro tre obiettivi strategici e le dieci azioni sono:

### 1 Protezione dei dati passa al digitale

- (1) promuovere le tecnologie per migliorare la privacy e protezione dati;
- (2) individuare soluzioni politiche trasversali;
- (3) aumentare la trasparenza, il controllo utente e la responsabilità nella grande elaborazione dei dati.

### 2 Creazione di partnership a livello globale

- (4) sviluppare una dimensione etica dati protezione;
- (5) che parla con una sola voce europea nel scena internazionale;
- (6) Protezione dei dati mainstreaming nella internazionali politiche.

### 3 L'apertura di un nuovo capitolo per la protezione dei dati dell'UE

- (7) adottare e attuare dati up-to-data norme di protezione;
- (8) aumentare la responsabilità degli organi dell'UE Col lect ING, l'utilizzo e la stor ing informazioni personali;
- (9) FACI li tat ing responsabile e informato politiche;
- (10) promuovere una conversazione matura sulla sicurezza e la privacy.



@EU\_EDPS

**# GEPD** immagina di strategia **#UNIONE EUROPEA** come non tutta una singola istituzione, diventando un faro e leader nei dibattiti che si ispira a livello globale

# 1. A boutthe GEPD

Il GEPD assicura che le istituzioni e gli organismi europei rispettino i diritti fondamentali alla vita privata e alla protezione dei dati, sia che sono coinvolti nel trattamento dei dati personali o per lo sviluppo di nuove politiche. Abbiamo tre principali campi di lavoro:

- **Supervisione:** Monitoriamo il trattamento dei dati personali da parte dell'amministrazione dell'UE e assicurare che siano conformi alle norme sulla protezione dei dati. I nostri compiti vanno da operazioni di trasformazione preliminare di controllo che possono presentare rischi specifici, per la gestione dei reclami e nella conduzione delle indagini.
- **Consultazione:** Si consiglia la Commissione europea, il Parlamento europeo e al Consiglio sulle proposte di nuove leggi e di altre iniziative legate alla protezione dei dati.
- **Cooperazione:** Noi lavoriamo con nazionale autorità per la protezione dei dati (DPA) per promuovere la protezione dei dati coerente in tutta l'UE. La nostra piattaforma principale per la cooperazione con le DPA è il Comitato europeo per la protezione dei dati (EDPB).

Fino al 11 dicembre 2018, le istituzioni europee hanno dovuto rispettare le norme sulla protezione dei dati di cui al regolamento 45/2001, che il GEPD era tenuto a rispettare. In data 11 dicembre 2018, queste regole sono state sostituite da regolamento 2018/1725.

Il regolamento 2018/1725 è equivalente alle istituzioni dell'Unione europea nello Il regolamento generale sulla protezione dei dati (GDPR). Il GDPR diventato pienamente applicabile in tutta l'UE il 25 maggio 2018 e stabilisce le norme di protezione dei dati che tutte le altre organizzazioni che operano nell'UE devono rispettare. Ha inoltre compiti al GEPD assicurare il segretariato del EDPB.

In aggiunta a questo, regole separate esistono relativa al trattamento dei dati personali per le attività operative svolte dalle forze dell'ordine dell'UE, Europol. Queste attività comprendono la lotta contro le forme gravi di criminalità e il terrorismo che colpisce più di uno Stato membro. La normativa di riferimento in questo caso è

regolamento 2016/794, che prevede anche la supervisione del GEPD di queste attività di trattamento dei dati.

## 1.1 SUPERVISIONE ED ESECUZIONE

Il GEPD mira a garantire che le istituzioni dell'UE non sono a conoscenza solo dei loro obblighi di protezione dei dati, ma può

anche essere responsabili di loro osservanza. Abbiamo diversi strumenti che possiamo utilizzare, i quali hanno lo scopo di favorire lo sviluppo di una cultura della protezione dei dati nelle istituzioni dell'UE:

- **controlli preventivi / consultazioni preventive :** Ai sensi del regolamento 45/2001, le istituzioni e gli organi dell'UE hanno dovuto informare il GEPD di qualsiasi procedura che prevede di effettuare che potrebbero aver posto un rischio per la protezione dei dati personali. Abbiamo esaminato le proposte e fornito raccomandazioni su come affrontare questi rischi. In base al nuovo regolamento, controlli preventivi non esistono più in questa forma. Tuttavia, in alcuni casi, le istituzioni e gli organi dell'UE devono consultare il GEPD dopo aver effettuato una valutazione d'impatto sulla protezione dei dati per una procedura rischiosa pianificata.
- **Denunce, contestazioni :** Ci occupiamo di reclami di singoli individui in materia di trattamento dei dati personali da parte delle istituzioni europee. Indaghiamo queste lamentele e decidere il modo migliore per gestirli.
- **Controllo del rispetto:** Il GEPD è responsabile di assicurare che tutte le istituzioni e gli organi dell'UE rispettino le norme sulla protezione dei dati. Monitoriamo la conformità in vari modi, anche attraverso visite e ispezioni.
- **Consultazioni sulle misure amministrative:** Noi emettere pareri su provvedimenti amministrativi in tema di trattamento dei dati personali, sia in risposta ad una richiesta specifica da un'istituzione dell'Unione europea o di nostra iniziativa.
- **Guida:** emettiamo Linee guida per le istituzioni dell'UE, progettati per aiutarli a meglio attuare i principi di protezione dei dati e conformi alle norme di protezione dei dati.
- **Lavorare con responsabili della protezione dei dati (DPO) :** Ogni istituzione e organo dell'Unione europea devono nominare un DPO, Chi è responsabile di assicurare che la loro istituzione è conforme alle norme sulla protezione dei dati. Lavoriamo a stretto contatto con gli RPD, fornendo loro formazione e supporto per aiutarli a svolgere efficacemente il loro ruolo.
- **La formazione delle istituzioni e degli organismi dell'UE:** Forniamo corsi di formazione per dirigenti e membri del personale delle istituzioni e degli organi dell'Unione europea. Ciò contribuisce a garantire il rispetto delle norme sulla protezione dei dati e il rispetto dei diritti e delle libertà personali, e per incoraggiare lo sviluppo di una cultura della protezione dei dati all'interno di ciascuna istituzione. Queste sessioni di formazione si concentrano su come aiutare le istituzioni ad andare oltre la conformità e dimostrare responsabilità.

## 1.2 POLITICA E CONSULTAZIONE

Il GEPD agisce come un consulente in materia di protezione dei dati per il legislatore dell'UE. Il nostro obiettivo è garantire che i requisiti di protezione dei dati sono integrate in tutte le nuove leggi, iniziative politiche e gli accordi internazionali. Questo viene fatto fornendo indicazioni sulla proposta di legge alla Commissione europea, in quanto istituzione, con il diritto di iniziativa legislativa, e il Parlamento europeo e il Consiglio, in qualità di co-legislatori. Usiamo diversi strumenti per aiutarci:

- **Commenti informali:** In linea con la prassi consolidata, la Commissione consulta il GEPD in modo informale prima di adottare una proposta con implicazioni per la protezione dei dati. Questo ci permette di fornire loro ingresso in una fase iniziale del processo legislativo, di solito sotto forma di osservazioni informali, che non sono pubblicati.
- **opinioni** : I nostri pareri formali sono disponibili sul nostro sito e sono pubblicati nella Gazzetta ufficiale dell'Unione europea. Li usiamo per evidenziare le nostre principali preoccupazioni sulla protezione dei dati e raccomandazioni sulle proposte legislative. Essi si rivolgono a tutte e tre le istituzioni dell'UE coinvolte nel processo legislativo.
- **formali Commenti** : Come le nostre opinioni, le nostre osservazioni formali affrontare le implicazioni per la protezione dei dati delle proposte legislative. Tuttavia, di solito sono più brevi e più tecnico, oppure solo affrontare alcuni aspetti della proposta. Noi li pubblicheremo sul nostro sito.
- **Casi giudiziari** : Siamo in grado di intervenire e offrire la nostra esperienza di protezione dei dati dinanzi ai giudici comunitari o per conto di una delle parti in un caso o su invito dei Tribunali.
- **Cooperazione con DPA nazionali:** Collaboriamo con le DPA nazionali attraverso l'EDPB, che garantisce l'applicazione coerente del GDPR attraverso linee guida, raccomandazioni e le migliori pratiche, le opinioni e le decisioni vincolanti, e fornisce alla Commissione europea con consigli su questioni relative alla protezione dei dati. Lavoriamo anche con DPA nazionali al fine di garantire un approccio coerente e coordinato per la supervisione di un certo numero di banche dati dell'UE.

## 1.3 MONITORAGGIO SVILUPPO TECNOLOGICO

Molte nuove tecnologie di processo dei dati personali in una serie di modi diversi e innovativi. Lo scopo di questi dati

trattamento è spesso quello di ottenere vantaggi economici o di altro. misure di protezione dei dati e privacy devono affrontare adeguatamente i nuovi sviluppi tecnologici. Questo farà sì che gli individui siano protetti dai rischi di queste nuove attività di trattamento dei dati potrebbe comportare.

Il GEPD monitora gli sviluppi tecnologici e del loro impatto sulla protezione dei dati e della privacy. La conoscenza e l'esperienza in questo settore ci permette di eseguire in modo efficace i nostri compiti di vigilanza e di consultazione. Questa capacità e competenza solo continuerà a crescere in importanza, a causa dei cambiamenti introdotti dal GDPR e il nuovo regolamento per le istituzioni e gli organi dell'UE. Le nostre attività comprendono:

- **Il monitoraggio e la risposta agli sviluppi tecnologici:** Abbiamo monitorato sviluppi tecnologici, gli eventi e gli incidenti e valutare il loro impatto sulla protezione dei dati. Questo ci permette di fornire consulenza su questioni tecniche, in particolare in relazione ai compiti di supervisione e consultazione del GEPD.
- **La promozione di ingegneria privacy:** Nel 2014 abbiamo lanciato il [Internet Privacy rete Ingegneria](#) (IPEN) in collaborazione con le DPA nazionali, sviluppatori e ricercatori dell'industria e del mondo accademico e rappresentanti della società civile. Il nostro obiettivo è quello di sviluppare sia pratiche di ingegneria che incorporano problemi di privacy e incoraggiano gli ingegneri per costruire meccanismi di privacy in servizi internet, gli standard e applicazioni.
- **Stabilire lo stato dell'arte nella protezione dei dati in base alla progettazione:** Con la GDPR e il regolamento 2018/1725 ora pienamente applicabile, è diventato un obbligo giuridico per tutti i controller per tener conto dello stato dell'arte della protezione dei dati tecnologia amica durante la progettazione, mantenere e gestire sistemi per il trattamento dei dati personali. Al fine di garantire l'applicazione coerente di questa regola in tutta l'UE, è importante che DPA stabilire una comprensione comune dello stato dell'arte e il suo sviluppo. Con questo in mente, il GEPD collabora con le autorità nazionali di vigilanza per valutare e valutare esistenti e lo sviluppo di opzioni tecnologiche e organizzative.
- **Tenere traccia di IT ai GEPD:** Come supervisore protezione dei dati per le istituzioni dell'Unione europea, dovremmo impostare il livello di osservanza della protezione dei dati. Abbiamo quindi continuamente controllare e migliorare la tecnologia utilizzata dai GEPD per garantire che funziona in modo efficace ed efficiente, pur rimanendo in linea con le esigenze di protezione dei dati.

## 2. 2018 - A n O verivew

Nel **Strategia GEPD 2015-2019**, Abbiamo delineare una visione di un'Unione europea che porta l'esempio nel dialogo globale sulla protezione dei dati e della privacy nell'era digitale. Ci siamo dati un ordine del giorno impegnativo e ambizioso, che abbiamo cercato di realizzare nel corso del mandato in corso.

Abbiamo fatto grandi passi avanti verso il raggiungimento di questi obiettivi nel 2018, un anno che potrebbe essere considerato fondamentale sia nella storia della protezione dei dati e nella storia del GEPD.

### 2.1 NUOVA LEGISLAZIONE PER UNA NUOVA ERA

Uno dei tre obiettivi di cui la nostra strategia era quella di aprire un nuovo capitolo per la protezione dei dati dell'UE. Lo sviluppo tecnologico si sta muovendo ad un ritmo rapido e il modo in cui viviamo, come individui e come società, sta anche cambiando rapidamente per ospitare questo. Logicamente, le norme sulla protezione dei dati dell'UE anche richiesto un aggiornamento, non mira a rallentare l'innovazione, ma a garantire che i diritti fondamentali delle persone siano protetti nell'era digitale.

Il 25 maggio 2018, una nuova normativa sulla protezione dei dati è diventato pienamente applicabile a tutte le aziende e le organizzazioni che operano negli Stati membri dell'Unione europea. Il

**Il regolamento generale sulla protezione dei dati (GDPR) ha segnato il primo passo per garantire una protezione completa ed efficace dei dati personali e della privacy per tutti gli individui nell'UE.**

Con questa nuova normativa è venuto l'istituzione del Comitato europeo per la protezione dei dati (EDPB) (**vedere la sezione 4.1.1**). Composto dello Stato membro dell'UE 28

**autorità per la protezione dei dati (DPA) e il GEPD**, questo nuovo organismo il compito di verificare l'attuazione coerente della GDPR in tutta l'UE. Accusato di assicurare il segretariato questo nuovo organo dell'UE, una quantità significativa del nostro tempo e fatica nei primi mesi del 2018 è andato in modo che il Consiglio sarebbe disposto a trattare con il suo pesante carico di lavoro dal primo giorno del nuovo regolamento. Abbiamo continuato a sostenere la segreteria EDPB amministrativamente durante tutto l'anno, così come partecipare pienamente come membro del Consiglio stesso.

Ci siamo trasferiti ancora un altro passo verso il raggiungimento di un quadro globale per la protezione dei dati con l'adozione di nuove regole per le istituzioni e gli organi dell'UE.

**regolamento 2018/1725** è entrato in vigore l'11 dicembre

2018, portando le regole per le istituzioni dell'UE, in linea con le norme stabilite nel GDPR (**vedere la sezione 4.1.2**).

In qualità di autorità di vigilanza per la protezione dei dati nelle istituzioni e negli organi dell'Unione europea, abbiamo affrontato la sfida significativa di garantire che tutti erano preparati per queste nuove regole. Nel 2017, abbiamo avviato una campagna di visite, la formazione sessioni e riunioni (**vedi figura 2**), Che si è intensificata nel corso del 2018. Questi sono stati finalizzati a sensibilizzare e sulle nuove regole e contribuire ad assicurare che le istituzioni dell'UE avevano le conoscenze e gli strumenti per metterli in pratica.

Un focus specifico di queste attività era favorire lo sviluppo di una cultura della **responsabilità all'interno delle istituzioni comunitarie**. Abbiamo voluto garantire che essi non solo sono conformi alle norme di protezione dei dati, ma che possono dimostrare tale conformità. Parte integrante di questo è stato la creazione di consapevolezza che il trattamento dei dati personali, anche quando fatto legalmente, può mettere i diritti e le libertà delle persone a rischio. Queste attività continueranno nel 2019, come ci sforziamo di garantire che le istituzioni dell'UE aprire la strada nell'applicazione delle nuove regole sulla protezione dei dati.

L'uso improprio dei dati personali per il monitoraggio e la finalità di profilazione e il ruolo della tecnologia nella nostra società è stato un argomento di notevole dibattito pubblico nel 2018. Il GEPD e la comunità la protezione dei dati in generale erano in prima linea di questo dibattito, con il GEPD contribuendo su due fronti principali: **tramite il nostro Opinione sulla manipolazione on-line e dei dati personali (vedere la sezione 4.4.17)** e il **nostro Opinione sulla Privacy by Design (vedere la sezione**

**4.1.4**).

Mentre il primo incentrato sulla necessità di estendere l'ambito di tutela degli interessi degli individui nella società digitale di oggi, quest'ultima sembrava per affrontare le nuove sfide derivanti dagli sviluppi tecnologici e legali. Dal punto di vista legale, la nuova generazione delle norme sulla protezione dei dati stabilite nel GDPR, la direttiva 2016/680 e il regolamento 2018/1725 sul trattamento dei dati personali da parte delle istituzioni UE richiede che i titolari tengono conto dello stato dell'arte in tecnica e misure organizzative per attuare i principi di protezione dei dati e misure di salvaguardia. Questo richiede anche che le autorità di vigilanza sono a conoscenza dello stato dell'arte in questo settore e che seguono il suo sviluppo. La cooperazione in questo settore è di fondamentale importanza al fine di garantire che tali principi siano applicati in modo coerente. **Internet Privacy rete Ingegneria (IPEN)**

( [vedere la sezione 4.4.16](#) ) Per favorire il dialogo tra i responsabili politici, le autorità di regolamentazione, industria, mondo accademico e della società civile su come le nuove tecnologie possono essere progettati a beneficio dell'individuo e della società.

Le nuove regole sulla protezione dei dati anche introducono il principio di **responsabilità** ( [vedere la sezione 4.4.2](#) ). Tutti i controllori, tra le istituzioni e gli organi dell'Unione europea, devono garantire che essi siano in grado di dimostrare la conformità con le nuove regole. Questo vale anche per la gestione e la governance delle infrastrutture e dei sistemi IT. Per contribuire a questo, abbiamo esteso il nostro catalogo di linee guida specifiche per includere, tra gli altri, [Linee guida per l'uso di servizi di cloud computing](#) da parte dell'amministrazione UE e [l'ulteriore linee guida per la gestione IT e IT governance](#) ( [vedere la sezione](#)

[4.4.3](#) ). Nel 2018, abbiamo anche iniziato un programma sistematico volto a verificare il rispetto degli organi dell'UE con le linee guida del GEPD.

## 2.2 trovare un equilibrio tra SICUREZZA E PRIVACY

1 Maggio 2018 ha segnato un anno da quando il GEPD ha assunto la responsabilità di vigilare sul trattamento dei dati personali per le attività operative a forze dell'ordine dell'UE, Europol. Uno dei punti di azione di cui la nostra strategia come parte integrante di aprire un nuovo capitolo per la protezione dei dati nell'UE è di promuovere una conversazione matura sulla sicurezza e la privacy. In qualità di agenzia dell'UE incaricata di garantire la sicurezza dell'UE, mentre la tutela dei diritti fondamentali alla vita privata e alla protezione dei dati, l'Europol è un grande esempio dei progressi che stiamo facendo in questo settore ( [vedere paragrafo 4.2](#) ).

Continuiamo a mantenere un forte rapporto con l'Europol di [Protezione dei dati](#) (DPO) e la funzione di protezione dei dati (DPF) Unità, che ci permette di anticipare eventuali problemi e pianificare le attività future ( [vedere la sezione 4.2.1](#) ). Abbiamo effettuato la nostra seconda ispezione delle attività di trattamento dei dati presso l'agenzia maggio 2018 ( [vedere la sezione 4.2.3](#) ) E ha continuato a fornire consulenza e trattare i reclami dove richiesto ( [vedere le sezioni 4.2.4 e 4.2.5](#) ).

La sicurezza delle frontiere dell'UE rimane un tema caldo e il legislatore europeo ha presentato diverse nuove proposte nel 2018 volte ad aumentare la sicurezza e migliorare la gestione delle frontiere. Pur riconoscendo la necessità di una maggiore sicurezza dell'UE, questo non deve andare a scapito della protezione dei dati e della privacy.

Facilitare politiche responsabile e consapevole è un altro dei punti di azione necessarie al fine di aprire un nuovo capitolo nella protezione dei dati nell'UE. Con questo in mente abbiamo elaborato diversi pareri sulla politica delle frontiere dell'UE proposto

nel 2018 ( [vedere la sezione 4.3.4](#) ). Uno di questi concentrati sul futuro della condivisione delle informazioni all'interno dell'UE, rivolgendosi proposte di due regolamenti che stabilire un quadro per l'interoperabilità **tra sistemi di informazione su larga scala UE** . Come le implicazioni di questa proposta di protezione dei dati e di altri diritti e libertà fondamentali sono incerte, lanceremo un dibattito su questo tema nei primi mesi del 2019 per assicurarsi che sono esplorate in dettaglio.

Abbiamo inoltre continuato la nostra stretta collaborazione con DPA per garantire un controllo efficace e coordinato su larga scala dell'UE database IT, utilizzato per sostenere le politiche dell'UE in materia di asilo, gestione delle frontiere, la cooperazione di polizia e la migrazione ( [vedere le sezioni 4.3.1 e 4.3.2](#) ).

## 2.3 PARTNERSHIP IN VIA DI SVILUPPO

Facilitare politiche responsabile e informato è tutt'altro che limitata al settore della politica delle frontiere e la sicurezza dell'UE, tuttavia. Nel 2018, il GEPD ha emesso 11 pareri, di cui due su richiesta del Consiglio, su questioni che vanno dalla giurisdizione in materia matrimoniale per l'interoperabilità dei sistemi di informazione su larga scala UE.

Abbiamo inoltre emesso 14 insiemi di osservazioni formali. Questi sono equivalenti alle opinioni, ma in genere più breve e più tecnico. Alcuni dei nostri commenti sono stati espressamente richiesto dal Parlamento europeo, o uno dei suoi Comitati, e non preoccupato delle proposte legislative iniziali, ma progetti di emendamento e risultati dei negoziati tra le co-legislatori.

Tenendo conto che anche noi affrontato con oltre 30 consultazioni informali su progetti di proposte da parte della Commissione, questi numeri dimostrano chiaramente la crescente necessità di, e la pertinenza della, consulenza di esperti indipendenti sulle implicazioni per la protezione dei dati di iniziative dell'UE, nonché un crescente interesse da attori istituzionali dell'UE. Non vediamo l'ora di continuare questa cooperazione reciprocamente vantaggiosa nei prossimi anni nel contesto dei poteri legislativi rafforzati di consultazione ai sensi del nuovo regolamento 2018/1725.

Abbiamo anche continuato i nostri sforzi per assicurare che le attività delle istituzioni europee sono svolte in conformità con le leggi vigenti sulla protezione dei dati, emissione prior- controllare Opinioni, indagare sulle denunce e monitorare la conformità attraverso i vari strumenti a **nostra disposizione** ( [vedere paragrafo 4.4](#) ).

La strategia si impegna al GEPD di creazione di partnership nel perseguimento di una maggiore convergenza di protezione dei dati a livello globale. Mentre flussi di dati a livello internazionale, attraverso le frontiere, le norme sulla protezione dei dati sono decise su una gran parte nazionali, e nella migliore delle ipotesi regionale, base.

Con questo in mente, noi continuiamo a lavorare con i nostri par part-regionali ed internazionali per la protezione dei dati tradizionale di accordi internazionali e assicurare una protezione coerente dei dati personali in tutto il mondo ( [vedere la sezione 4.5.2](#) ).

Ci sono anche coinvolti in discussioni sui risultati di adeguatezza. Questi accordi sono fatti da parte della Commissione europea, a nome degli Stati membri dell'Unione europea, e prevedono il trasferimento dei dati da paesi dell'Unione europea verso i paesi extra-UE i cui dati protezione regole sono considerati per fornire una protezione adeguata. Specificamente, in

2018, abbiamo contribuito alla seconda revisione congiunta dell'accordo UE-USA Privacy Shield e il parere EDPB su un accordo adeguatezza proposto con il Giappone ( [vedere la sezione 4.5.1](#) ).

## 2.4 DIGITALE ETICA E LA CONFERENZA INTERNAZIONALE

Abbiamo lanciato il [GEPD Ethics Initiative](#) di nuovo nel 2015, come parte del nostro impegno per forgiare partnership globali. Abbiamo voluto generare una discussione globale su come i nostri diritti e valori fondamentali possono essere accolti nell'era digitale.

Tre anni e l'etica digitali è ora molto nell'agenda internazionale.

Abbiamo iniziato 2018 con la pubblicazione del [Rapporto Etico Advisory Group](#) ( [vedere la sezione 4.6.1](#) ). Il Rapporto è uno strumento utile per aiutarci a capire come la rivoluzione digitale ha cambiato il modo in cui viviamo la nostra vita, sia come individui che come società. Si delinea anche i cambiamenti e le sfide questo implica per la protezione dei dati. Da qui, siamo stati in grado di espandere la nostra richiesta di raggiungere un pubblico molto più ampio, attraverso una consultazione pubblica avviata all'inizio dell'estate 2018 ( [vedere la sezione 4.6.2](#) ). I risultati della consultazione hanno rivelato l'importanza dell'etica in movimento in avanti e hanno chiesto DPA di svolgere un ruolo attivo in questo.

Tuttavia, è stato il [Conferenza internazionale di protezione dei dati e della privacy](#) , Soprannominato il *Olimpiadi di protezione dei dati* dal GEPD Giovanni Buttarelli, che in realtà ha lanciato la discussione sull'etica digitali su nell'agenda internazionale.

La sessione pubblica della Conferenza internazionale focalizzata su *Debating Etica: Dignità e rispetto in Data Driven Life*. Con oltre 1000 persone provenienti da una varietà di differenti ambiti di provenienza, nazionalità e professioni presenti, relatori di alto profilo e una notevole copertura mediatica, l'evento è servito a promuovere il dibattito sulla questione e mettere nuove questioni etiche e legali ai primi posti nell'agenda del DPA e altri attraverso il mondo.

Il GEPD è ora visto come un leader in questo settore e lavorerà duramente per progredire il dibattito ( [vedere la sezione 4.7](#) ).

## 2.5 AMMINISTRAZIONE INTERNA

Con la nostra ruolo e le responsabilità in espansione, una buona amministrazione interna è stata più importante che mai per garantire che siamo in grado di raggiungere i nostri obiettivi.

Le risorse umane GEPD, bilancio e amministrazione Unità (HRBA) affrontato due particolarmente grandi lavori preparatori nel 2018 ( [vedi sezione 7.2](#) ). Il lavoro sui preparativi per il nuovo segretariato EDPB intensificato in modo significativo al fine di garantire che il Consiglio era amministrativamente e logisticamente pronti per iniziare a lavorare il 25 maggio 2018. Tra le altre cose, questo ha comportato assicurando che tutti i membri del personale EDPB erano soggetti alle stesse regole lavorare per il GEPD e in grado di beneficiare degli stessi diritti.

In vista del nuovo regolamento sulla protezione dei dati per le istituzioni dell'Unione europea, abbiamo avuto anche per garantire che tutte le decisioni GEPD HR rispettate le nuove regole. Abbiamo quindi intrapreso una revisione completa di tutte le attività di trattamento dei dati GEPD HR e rivisto il nostro approccio a seconda delle necessità.

Oltre a una serie di iniziative volte a migliorare le nostre politiche HR, abbiamo lanciato un nuovo concorso per creare un pool di esperti di protezione dei dati altamente qualificati per soddisfare le nostre esigenze di reclutamento future. Come ci muoviamo nel 2019, il nostro scopo principale è quello di garantire un ambiente di lavoro efficiente e piacevole per tutti coloro che lavorano presso il GEPD.

## 2.6 COMUNICARE PROTEZIONE DEI DATI

L'importanza delle attività di comunicazione del GEPD è aumentato considerevolmente negli ultimi anni ( [vedi sezione 7.1](#) ). Una comunicazione efficace è essenziale per garantire che siamo in grado di raggiungere gli obiettivi fissati nella nostra strategia. Se il nostro lavoro non è visibile, non può avere l'effetto desiderato.

Oltre a consolidare i nostri sforzi per migliorare e aumentare l'impatto della nostra presenza online, abbiamo lanciato ed eseguito due campagne di comunicazione. I nostri sforzi di comunicazione per la Conferenza Internazionale 2018 non solo ha contribuito a garantire che la conferenza in sé è stato un successo, ma che il dibattito sull'etica digitali hanno raggiunto il più ampio pubblico possibile.

Nel mese di dicembre 2018, abbiamo rivolto la nostra attenzione al nuovo regolamento sulla protezione dei dati per le istituzioni dell'UE. La nostra campagna di comunicazione è stato progettato per integrare

e rafforzare le attività di sensibilizzazione in corso, si era rivolto non solo a membri del personale dell'UE, ma anche ad assicurare che le persone al di fuori delle istituzioni dell'UE erano a conoscenza delle nuove regole e come li potrebbero influenzare.

Con la presenza globale e l'influenza dei GEPD solo destinati ad aumentare, ci aspettiamo un altro anno impegnativo avanti nel 2019.

## 2.7 DATI SALIENTI 2018

Usiamo una serie di indicatori chiave di performance (KPI) per aiutarci a monitorare le nostre prestazioni. Questo assicura che siamo in grado di regolare le nostre attività, se necessario, per aumentare l'impatto del nostro lavoro e l'efficienza del nostro utilizzo delle risorse. Questi KPI riflettono gli obiettivi strategici e piano d'azione definite nella nostra strategia 2015-2019.

Il quadro di valutazione KPI di seguito contiene una breve descrizione di ogni KPI ed i risultati al 31 dicembre 2018. Nella maggior parte dei casi, questi risultati sono misurati contro obiettivi iniziali.

Nel 2018, abbiamo incontrato o superato, in alcuni casi in modo significativo, gli obiettivi fissati nella maggior parte dei nostri KPI. Questo dimostra che l'attuazione dei pertinenti obiettivi strategici è a buon punto e non sono necessari interventi correttivi.

In due casi non abbiamo risultati del monitoraggio. Nel caso di KPI 6, nel corso del 2018 abbiamo optato per monitorare e dare priorità le nostre attività politiche in relazione alle azioni prioritarie relative delineati nella nostra strategia, invece di pubblicare un elenco di priorità. Abbiamo preso questa decisione perché abbiamo ritenuto che questo era un modo più efficace per garantire che incontriamo gli obiettivi fissati nella strategia GEPD.

Nel caso di KPI 7, non siamo attualmente in grado di misurare con precisione il numero di visitatori al sito web del GEPD, a causa di un cambiamento nella politica di biscotto e di monitoraggio sul nostro sito web ( [vedere la sezione 7.1.1](#) ). Questo cambiamento è volto a garantire che gli utenti del nostro sito potranno consapevolmente *opt-in* ad avere la loro attività on-line seguita sul sito web del GEPD. Sarà quindi garantire che il sito web è la protezione dei dati friendly possibile. Per questo motivo i risultati per KPI 7 non sono completi.

Il target per KPI 4 è riadattato ogni anno, in conformità con il ciclo legislativo.

INDICATORE CHIAVE DI PRESTAZIONE		RISULTATI AL 31.12.2018	TARGET 2018
Obiettivo 1 - Protezione dei dati passa al digitale			
KPI indicatore interno 1	Numero di iniziative di promozione delle tecnologie per migliorare la privacy e protezione dei dati organizzati o co-organizzato dal GEPD	9	9 iniziative
KPI 2 Indicatore interna ed esterna	Numero di attività incentrate su soluzioni politiche trasversali (interna ed esterna)	8	8 iniziative
Obiettivo 2 - creazione di partnership a livello globale			
Indicatore interno 3 KPI	Numero di casi trattati a livello internazionale (EDPB, CoE, OCSE, GPEN, Conferenze Internazionali) per i quali GEPD ha fornito un sostanziale contributo scritto	31	10 casi
Obiettivo 3 - L'apertura di un nuovo capitolo per la protezione dei dati dell'UE			
Indicatore KPI 4 esterno	Livello di interesse delle parti interessate (COM, PE, del Consiglio, DPA, etc.)	15	10 consultazioni
Indicatore KPI 5 esterno	Livello di soddisfazione dei / controllori di DPO / del DPC sulla cooperazione con GEPD e di orientamento, compresa la soddisfazione delle persone interessate da addestramento	95%	70%
KPI indicatore interno 6	Tasso di esecuzione dei casi nella lista di priorità GEPD (come regolarmente aggiornato) in forma di osservazioni informali e pareri formali	N / A	N / A
Abilitanti - Comunicazione e gestione delle risorse			
KPI 7 Indicatore esterno Composite	Numero di visite al sito web del GEPD Numero di seguaci sul conto GEPD Twitter	N / A 14.000	Raggiungere 195715 (2015 risultati) visite 9407 seguaci (2017 risultati) + 10%
KPI indicatore interno 8	Livello di soddisfazione del personale	75%	75%
Indicatore interno KPI 9	esecuzione del bilancio	93,8%	90%

Figura 1. tabella di analisi GEPD KPI

## 3. Main Objectives for 2019

I seguenti obiettivi sono stati selezionati per il 2019 all'interno del complesso **Strategia per 2015-2019**. Faremo una relazione sui risultati del 2019 Annual Report.

### Garantire la corretta applicazione del regolamento 2018/1725

Il nuove regole sulla protezione dei dati per l'UE istituzioni e gli organismi si applica integralmente in data 11 dicembre 2018 ( [vedere la sezione 4.1.2](#) ). Nel 2019, continueremo la nostra campagna per garantire che sia coloro che lavorano per le istituzioni dell'UE e quelli che non sono in grado di sviluppare una migliore comprensione dei requisiti del nuovo regolamento e una maggiore consapevolezza dei rischi associati alla trattamento dei dati personali dati.

All'interno delle istituzioni dell'Unione europea, continueremo la nostra attenzione sulla necessità di incoraggiare lo sviluppo di una cultura della **responsabilità**. È quindi indispensabile fornire **Responsabili della protezione dei dati (DPO)**, membri della direzione e del personale dell'Unione europea con le conoscenze e gli strumenti per andare oltre la semplice conformità, per garantire che essi sono anche in grado di dimostrare tale conformità.

### Una nuova base giuridica per le attività di politica e di consultazione

Regolamento 2018/1725 rafforza il ruolo del GEPD nelle nostre attività di politica e di consultazione. La Commissione europea è ora esplicitamente richiesto di consultare il GEPD in casi specifici e noi dobbiamo fornire loro consulenza entro otto settimane dalla ricezione della loro richiesta. La nuova normativa prevede anche la possibilità di emettere pareri congiunti con il Consiglio europeo per la protezione dei dati (EDPB).

Nel 2019, lavoreremo con la Commissione e l'EDPB per garantire che le procedure appropriate sono messe in atto per supportare queste nuove disposizioni e noi rivedere e aggiornare le nostre regole interne e di altri documenti di orientamento rilevanti. Ci sarà anche restare a disposizione della Commissione europea, il Parlamento europeo e al Consiglio di fornire consulenza formale o informale, in qualsiasi punto del processo decisionale.

### Fornire orientamenti sulle necessità e proporzionalità

Nel 2019, completeremo il nostro lavoro sulla fornitura di una metodologia per il legislatore europeo da seguire quando

valutare la necessità e la proporzionalità delle misure legislative che hanno un impatto sui diritti fondamentali alla vita privata e alla protezione dei dati. In particolare, svilupperemo Orientamenti in materia di proporzionalità, completando il lavoro che abbiamo iniziato con la pubblicazione del nostro **necessità Toolkit** nel mese di aprile 2017. In tal modo, ci proponiamo di fornire alle istituzioni dell'UE, con una struttura che li aiuterà ad adottare un approccio proattivo all'implementazione salvaguardie per la protezione dei dati nella politica europea.

### Facilitare più ampio dibattito sull'interoperabilità

Nel nostro 2018 **Opinione sull'interoperabilità tra l'UE sistemi IT su larga scala** ( [vedere la sezione 4.3.4](#) ) Abbiamo chiamato per un più ampio dibattito sul futuro di questi sistemi, la loro governance e su come salvaguardare i diritti fondamentali in questo settore. Lanceremo questo dibattito nel 2019, con un gruppo ad alto livello sul tema a Computer annuali, Privacy e Conferenza sulla protezione dei dati (CPDP), che si terrà a Bruxelles dal 30 gennaio-1 febbraio 2019.

Il nuovo regolamento 2018/1725 prevede un unico modello di controllo coordinato per i sistemi dell'UE su vasta scala IT e organi dell'UE, uffici e agenzie, che devono essere effettuati dal GEPD e dalle autorità di vigilanza nazionali ( [vedere la sezione 4.3.2](#) ). A fianco dei nostri partner nelle DPA nazionali, rifletteremo sul futuro del controllo coordinato nel corso del 2019.

### Informazioni Protezione

Il nuovo regolamento per la protezione dei dati nelle istituzioni dell'UE introduce nuovi concetti che sottolineano l'importanza della sicurezza delle informazioni. Questi includono obbligatorie le notifiche di violazione dei dati e l'uso di pseudonimi come misura di sicurezza riconosciuto.

Per tenere conto di questo, avremo bisogno di aumentare la nostra capacità e la competenza di sorvegliare e valutare le misure adottate dalle istituzioni dell'UE per ottenere la conformità. Dobbiamo anche essere in grado di reagire rapidamente alle notifiche di violazioni dei dati e altri incidenti di sicurezza, al fine di garantire che qualsiasi effetto negativo sui diritti fondamentali delle persone è limitata. Noi cont inue per condurre

ispezionare ioni focalizzata sulla aspetti tecnologici, in particolare quelle relative ai sistemi IT su larga scala ( [vedere la sezione 4.3.1](#) ) E nel settore della sicurezza e delle forze dell'ordine.

## Gestire la transizione alla vigilanza Eurojust

Con la nostra funzione di vigilanza presso l'Europol ormai ben consolidata ( [vedere paragrafo 4.2](#) ), Nel 2019 il GEPD assumerà il compito di vigilare trattamento dei dati personali in un'altro agenzia dell'Unione europea che operano nel settore della giustizia e degli affari interni: Eurojust ( [vedere la sezione 4.4.13](#) ).

Un nuovo quadro giuridico per l'Eurojust, che include nuove regole sulla protezione dei dati specifici per le attività dell'agenzia, è stato adottato il 6 novembre 2018. Esso prevede un ruolo di supervisione deve essere eseguito dal GEPD. Per preparare per il nostro nuovo ruolo, personale del GEPD organizzerà corsi di formazione interni ed esterni relativi alla vigilanza Eurojust, il tutto finalizzato a garantire che siamo pronti a prendere il nostro nuovo ruolo alla fine del 2019.

## Implementare la protezione dei dati di progettazione e di default nelle istituzioni dell'UE

Secondo le nuove regole sulla protezione dei dati, le istituzioni dell'UE hanno l'obbligo di attuare i principi della protezione dei dati per la progettazione e per impostazione predefinita quando sviluppare e gestire sistemi di elaborazione dati ( [vedere la sezione](#)

[4.1.4](#) ). Saremo quindi aumentare i nostri sforzi per individuare e promuovere soluzioni tecnologiche pratiche nel 2019. Ciò comporterà regolarmente monitorare gli sviluppi delle TIC al fine di fornire orientamento e formazione sulla realizzazione tecnica di protezione dei dati.

## Guida alla tecnologia e protezione dei dati

Nel 2018, abbiamo pubblicato linee guida in materia di protezione dei dati personali in [IT governance e gestione](#) , [cloud computing](#) e [le notifiche di violazione dei dati](#) . Nel 2019, noi emetteremo linee guida aggiornate volto a migliorare la responsabilità nel settore IT, e fornire consulenza politica in materia di tecnologie o metodologie specifiche, con particolare attenzione sulla sicurezza.

Per assicurare la coerenza con la consulenza e la pratica di altri [autorità per la protezione dei dati](#) (DPA), seguiremo la guida del EDPB su questi temi e contribuire al loro lavoro sulle linee guida armonizzate.

Continueremo anche a collaborare con i nostri partner internazionali sulla tecnologia e la protezione dei dati, tra cui la Conferenza internazionale di protezione dei dati e della privacy (ICDPPC) e dei suoi gruppi di lavoro e del gruppo di lavoro internazionale sui dati

Protezione e Telecomunicazioni (IWGDPT, noto come il Gruppo di Berlino) ( [vedere la sezione 4.5.2](#) ).

Attraverso le ispezioni e indagini, continueremo i nostri sforzi per valutare la conformità di protezione dei dati all'interno delle istituzioni europee. Ove possibile, faremo il possibile per portare questi a distanza, dal laboratorio GEPD.

## Sostenere la privacy su Internet Network Engineering (IPEN)

Come una rete di tecnologia e di esperti di privacy dal DPA, industria, **mondo accademico e della società civile**, **IPEN svolgerà un ruolo importante** nel tradurre i principi di protezione dei dati in requisiti ingegneristici. Sosterremo la rete a intensificare i suoi sforzi per promuovere la tecnologia privacy amichevole e tecniche di ingegneria privacy-aware. In particolare, ci concentreremo i nostri sforzi sulla tradurre il principio della privacy by design in requisiti di ingegneria e a facilitare uno scambio tra ingegneri ed esperti di privacy su soluzioni tecniche per questioni di privacy, attraverso workshop e presentazioni in occasione di eventi pubblici.

Il nuovo obbligo giuridico di applicare il principio della protezione dei dati in base alla progettazione e per impostazione predefinita nella progettazione e gestione di sistemi informatici utilizzati per il trattamento dei dati personali ha aumentato l'importanza del lavoro in questo settore, in particolare per quanto riguarda la determinazione dello stato dell'arte e il suo sviluppo come punto di riferimento per le attività di supervisione e di applicazione.

## costante cooperazione con i partner internazionali dell'UE e

Con la nuova legislazione UE ora pienamente applicabile, la cooperazione con i nostri partner di protezione dei dati all'interno e all'esterno dell'UE è più importante che mai. Cooperazione con lo Stato DPA membri continuerà a molti livelli e all'interno del EDPB in particolare, dove la nostra attenzione sarà focalizzata sulla partecipazione attiva ha continuato con il lavoro delle disposizioni chiave sottogruppo e come membro del team di redazione con il compito di elaborare emendamenti alla EDPB Regole di procedura.

Continuando il nostro lavoro con le organizzazioni internazionali, organizzeremo un workshop a metà del 2019, che si svolgerà a Parigi. I nostri sforzi per promuovere un dialogo a livello internazionale con le autorità, le organizzazioni e altri gruppi provenienti da fuori l'UE anche restare una priorità.

## Mantenere lo slancio per l'iniziativa etica

Dopo il successo della [2018 Conferenza internazionale di protezione dei dati e della privacy](#) (vedere le sezioni [4.6.3](#) e [4.7](#)), La nostra sfida è ora quella di garantire che questo slancio continui. Ad un evento che si terrà come parte del computer, Privacy e protezione dei dati (CPDP) Conferenza all'inizio del 2019, lanceremo diverse nuove attività volte a fare proprio questo. Questi includeranno:

- una serie di conversazioni pubbliche nel formato di chiamate in conferenza, discussioni o podcast web-streaming, con esperti dei vari settori, tra cui DPA;

- pezzi di parere da leader di pensiero sul tema dell'etica digitali, che sarà pubblicato on-line;
- un nuovo parere del GEPD sull'etica, sulla nostra [2015 Parere](#) e il [Rapporto Etico Advisory Group](#) .
- un evento collaterale di etica che si svolgeranno nel corso della Conferenza internazionale di protezione dei dati e della privacy 2019.

Attraverso queste attività, speriamo di fare continui progressi verso il raggiungimento di un consenso internazionale sull'etica digitali.

## 4. 2 018 ighlights H

Il nuovo quadro normativo è stato, ancora una volta, un focus significativo del nostro lavoro nel 2018. Garantire il successo del lancio del Comitato europeo per la protezione dei dati (EDPB) e contribuire al lavoro del Consiglio durante tutto l'anno è stato un aspetto di questo. Il tempo considerevole e sforzo investito nella preparazione delle istituzioni dell'UE per la [nuove regole sulla protezione dei dati](#)

applicabile al loro lavoro è stato un altro. Abbiamo anche continuato a spingere per il legislatore europeo ad adottare il nuovo regolamento tanto necessario sulla e-privacy.

Il nostro ruolo di supervisore protezione dei dati per l'autorità di polizia dell'Unione europea, Europol, è ormai ben consolidata. Dopo più di un anno in questo ruolo, ora abbiamo un forte rapporto di lavoro con i nostri omologhi presso l'Europol e stiamo facendo buoni progressi nei nostri sforzi per trovare il giusto equilibrio tra sicurezza e la privacy quando si tratta di trattamento dei dati a fini di applicazione della legge.

Trovare il giusto equilibrio tra sicurezza e privacy è anche una preoccupazione in altre aree della politica dell'UE. Abbiamo risposto a diverse nuove proposte politiche nel 2018, volto a mantenere i confini dell'UE sicuro. Nel frattempo, abbiamo continuato a lavorare a stretto contatto con le istituzioni europee e le autorità nazionali al fine di garantire un controllo efficace e coordinato del trattamento dei dati personali in esistenti [Sistemi di controllo di frontiera](#).

Tuttavia, non è solo la politica delle frontiere dell'UE, che ha implicazioni per la protezione dei dati. Nel 2018 abbiamo pubblicato opinioni su una vasta gamma di argomenti diversi, tutti volti ad assicurare che le proposte avanzate dal legislatore comunitario adeguatamente rispettare e proteggere i diritti alla [protezione dei dati e della privacy](#). Un esempio di questo è stato il nostro [Opinione](#) sulla interoperabilità delle banche dati su larga scala dell'UE.

Nel nostro ruolo di supervisore della protezione dei dati, abbiamo risposto alle lamentele, ha effettuato accertamenti e rilasciato [precedenti controlla opinioni](#). Al fine di aiutare le istituzioni dell'UE garantiscono il rispetto delle norme pertinenti. Abbiamo intensificato la nostra stretta collaborazione con [Protezione dei dati antigelof \(DPO\)](#) e gli altri membri f STAF UE, l'organizzazione di incontri, visite e sessioni di formazione tutte finalizzate alla loro preparazione per le nuove regole.

Abbiamo continuato a lavorare a stretto contatto con i nostri partner protezione dei dati e altri in tutto il mondo, nei nostri sforzi per stabilire un approccio più internazionale per i dati

politica di protezione. Come negli anni precedenti, abbiamo contribuito pienamente alle discussioni europee e internazionali in materia di protezione dei dati, collaborando con il Consiglio d'Europa per lo sviluppo di una nuova convenzione internazionale sulla protezione dei dati, tra le altre cose. Abbiamo monitorato e fornito consigli sui trasferimenti internazionali di dati e abbiamo fatto ulteriori progressi nel nostro lavoro con le organizzazioni internazionali.

etica digitale fornito un altro forum per la cooperazione internazionale, in quanto abbiamo aumentato i nostri sforzi per incoraggiare il [dibattito sul tema in tutto il mondo e in tutte le discipline](#). Il [2018 Conferenza internazionale di protezione dei dati e della privacy](#) dimostrato un traguardo significativo per la [GEPD Ethics Initiative](#), Avviare il dibattito sulla scena internazionale.

Il raggiungimento dei nostri obiettivi e di vivere all'altezza delle aspettative, non sarebbe possibile senza il supporto della nostra Segreteria. Le loro attività sono essenziali per garantire l'efficienza amministrativa del GEPD e fare in modo che il nostro lavoro raggiunge il pubblico cui è destinato.

Come l'attuale mandato del GEPD si muove nel suo ultimo anno, noi guardiamo al 2019 come occasione per consolidare e costruire su nostri risultati, al fine di assicurare che siamo in grado di raggiungere gli obiettivi che ci siamo posti nel [strategia GEPD](#). Con l'importanza della protezione dei dati ormai saldamente affermata nell'agenda internazionale, non abbiamo alcun dubbio che il GEPD continuerà a servire come un importante punto di riferimento per tutti la protezione dei dati le cose nell'Unione europea.

### 4.1 PREPARAZIONE PER UN NUOVO QUADRO LEGISLATIVO

2018 ha segnato l'inizio di una nuova era nella protezione dei dati nell'UE. Il 25 maggio 2018, il [Il regolamento generale sulla protezione dei dati \(GDPR\)](#) è diventato pienamente applicabile a tutte le imprese, organizzazioni e istituzioni che operano nell'Unione europea. La nuova normativa ha inoltre istituito il Comitato europeo per la protezione dei dati (EDPB), un nuovo organismo comunitario il compito di facilitare la [cooperazione tra l'UE del cittadino autorità per la protezione dei dati \(DPA\)](#). Il GEPD partecipa a pieno titolo alle attività del Consiglio e fornisce la sua segreteria.

Due giorni prima del lancio del GDPR, il legislatore europeo ha raggiunto un accordo su norme equivalenti per le istituzioni, gli organismi e le agenzie. Questo

legislazione, che definisce anche il ruolo e le competenze del GEPD come l'autorità di vigilanza per le istituzioni dell'Unione europea, è diventato pienamente applicabile l'11 dicembre

2018. In preparazione per le nuove regole, abbiamo investito energie e risorse significative nel garantire che le istituzioni dell'UE sono stati adeguatamente preparati, fornendo corsi di formazione per tutti i livelli di gestione e personale dell'UE e la produzione di una guida di riferimento, tra le altre attività.

Questi due nuovi regolamenti, insieme con la direttiva sul diritto sulla protezione dei dati esecuzione applicabili dal 6 maggio 2018, rafforzano la posizione dell'UE come leader mondiale nella protezione dei dati e la pratica della privacy. Hanno anche andare un lungo cammino verso ci aiuta a raggiungere l'obiettivo strategico di aprire un nuovo capitolo per la protezione dei dati dell'UE, di cui la [Strategia GEPD 2015-2019](#).

Tuttavia, un pezzo di questo puzzle normativo è ancora mancante. Solo mediante la conclusione di un nuovo regolamento e-privacy, che riflette in modo accurato e sostiene i principi delineati nella GDPR, possiamo garantire che i diritti fondamentali della protezione dei dati e della privacy siano pienamente rispettati. In linea con i nostri impegni di strategia, continueremo a sostenere gli sforzi del legislatore europeo a venire ad un accordo su un nuovo regolamento ePrivacy entro la fine del corrente legislatura UE maggio 2019.



 @EU\_EDPS

Protocollo d'intesa firmato tra Comitato europeo per la protezione dei dati (EDPB) e Garante europeo della protezione dei dati (GEPD) durante la prima riunione plenaria EDPB oggi delineando modo in cui EDPB e GEPD coopereranno

[@Buttarelli\\_G](#) & Andrea Jelinek  
[#GDPRDay](#) <https://t.co/piKtWb5Yys>

#### 4.1.1 L'EDPB si mette al lavoro

Il 25 maggio 2018, il giorno in cui il GDPR divenuto pienamente applicabile per tutte le imprese e le organizzazioni che operano nell'UE, l'EDPB iniziato i suoi lavori.

Fondata sotto il GDPR, il Consiglio sostituisce il gruppo di lavoro Articolo 29 (WP29) come il forum per la cooperazione tra le DPA del 28 Stati membri e il GEPD. Ci vuole anche su molti nuovi compiti, volte a garantire l'applicazione coerente del GDPR in tutta l'UE. In aggiunta a questo, il Consiglio è in grado di emettere decisioni, le linee guida e le dichiarazioni su una vasta gamma di argomenti.

Nell'ambito del nuovo quadro giuridico, il GEPD ha il compito di assicurare il segretariato del EDPB. Operativo dal primo giorno del GDPR, la segreteria non solo fornisce supporto amministrativo e logistico per l'EDPB, ma svolge anche compiti di ricerca e analisi in materia. Oltre a fornire la segreteria, il GEPD è membro a pieno titolo del consiglio di amministrazione e ha partecipato alle cinque EDPB riunioni plenarie che hanno avuto luogo tra maggio e dicembre 2018.

Gran parte del lavoro svolto dalla EDPB avviene all'interno di sottogruppi, ognuno dei quali si riferisce ad una specifica area connessa alla protezione dei dati. Questi includono disposizioni chiave della GDPR, trasferimenti internazionali, la tecnologia e le questioni finanziarie, tra molti altri.

rappresentanti GEPD hanno partecipato alle riunioni dei sottogruppi che hanno avuto luogo nel 2018. Tra una serie di argomenti, i membri hanno condiviso le loro opinioni sui meccanismi di consistenza e di cooperazione volti a armonizzare le prassi di protezione dei dati in tutta l'UE, compreso il funzionamento del cosiddetto meccanismo One Stop Shop. È stato anche discusso le prestazioni del sistema di informazione del mercato interno (IMI), la piattaforma informatica utilizzata per lo scambio di informazioni su questioni transfrontaliere, così come le sfide e le tipologie di domande ricevute da DPA sotto il GDPR. La maggior parte delle DPA ha registrato un notevole aumento del numero di reclami ricevuti dal 25 maggio 2018.

Il Consiglio ha adottato il 26 [opinioni](#) nel 2018, che istituisce un elenco di casi in cui le organizzazioni devono svolgere la protezione dei dati valutazioni d'impatto (DPIAs). Questi elenchi sono uno strumento importante per garantire l'applicazione coerente del GDPR in tutta l'UE. Un [Opinione](#) sul nuovo regolamento eEvidence è stato inoltre adottato, così come vari altri lettere e documenti, tra cui orientamenti per il [campo di applicazione territoriale del GDPR](#), sopra

[GDPR cert t se icat ione](#), Sull'accreditamento e sulla [deroghe per trasferimenti internazionali](#). Il 5 dicembre

2018, l'EDPB inoltre adottato un parere in merito al progetto UE-Giappone decisione di adeguatezza per i trasferimenti internazionali di dati ([vedere la sezione 4.5.1](#)).

Al fine di fronteggiare l'aumento del carico di lavoro del Consiglio di Amministrazione, il numero di riunioni plenarie è destinata a raddoppiare in

2019. Mentre entriamo in una nuova era, in pratica, la protezione dei dati, ci auguriamo di poter continuare e intensificare la cooperazione con i nostri compagni DPA attraverso il neo costituito EDPB.

#### 4.1.2 Il regolamento protezione dei dati per le istituzioni dell'UE



#### regolamento 2018/1725

Mentre il GDPR si applica a tutte le aziende e le organizzazioni che trattano dati personali all'interno dell'UE, non si applica alle istituzioni dell'UE, che devono aderire a separate regole.

Il 23 maggio 2018, due giorni prima della GDPR diventato pienamente applicabile, rappresentanti del Parlamento europeo e il Consiglio hanno concordato un nuovo regolamento sul trattamento dei dati personali da parte delle istituzioni dell'UE e gli altri organi dell'UE. Il testo è stato adottato in occasione della sessione plenaria del Parlamento europeo il 13 settembre 2018 e in Consiglio un mese dopo. Il 23 ottobre 2018, è stato firmato dai presidenti del Parlamento europeo e il Consiglio dell'UE. Pubblicata nella Gazzetta ufficiale dell'Unione europea, come [regolamento 2018/1725](#) il 21 novembre

2018, le nuove regole si applica integralmente in data 11 dicembre 2018.

E' fondamentale che, quando si tratta con le istituzioni dell'Unione europea, tutti i dipendenti e cittadini dell'UE sono in grado di godere degli stessi diritti rafforzati come farebbero sotto il GDPR. Il nuovo regolamento, quindi, integra le norme sulla protezione dei dati per le istituzioni europee, in precedenza di cui [regolamento 45/2001](#) , In linea con gli elevati standard previsti dalla GDPR.

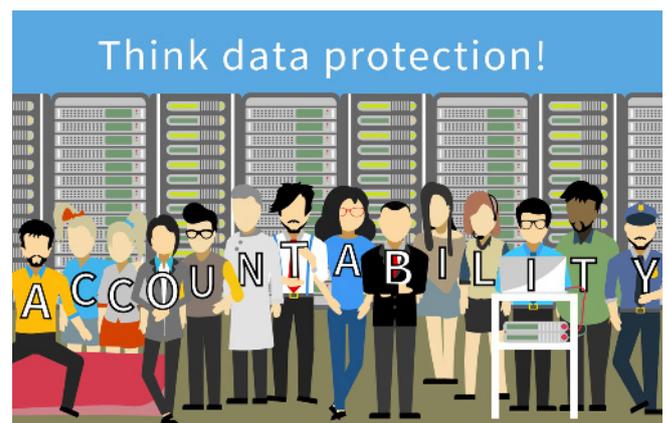
Il regolamento 2018/1725 comprende anche un capitolo che specificava sul trattamento dei dati personali operativi da parte delle agenzie dell'UE che lavorano nel campo della legge e della cooperazione giudiziaria in materia penale, come Eurojust. Queste regole sono in linea con quelli previsti nella direttiva di applicazione di legge che, come il GDPR, è divenuto applicabile maggio

2018. Le agenzie che operano in questo settore hanno la possibilità di sviluppare norme più dettagliate sul tema e li includono nei loro atti fondatori. Questo permetterà alle agenzie per tenere conto di eventuali particolarità del loro modo di operare.

Per ora, il trattamento dei dati personali operative di Europol e l'Ufficio del Pubblico Ministero europeo rimane al di fuori del campo di applicazione di queste nuove regole, con la Commissione europea ha di riesaminare la situazione entro il 2022.

#### Coordinare il passaggio al nuovo regolamento

In previsione delle nuove regole, abbiamo lavorato a stretto contatto con [Data Protection Officers \(DPO\)](#) e altri rappresentanti di tutte le istituzioni, gli organi e le agenzie dell'UE in tutto il 2017 e il 2018 per assicurarsi che sono stati preparati. Queste attività inclusi laboratori interattivi organizzati nell'ambito dei nostri incontri semestrali con gli RPD ( [vedere la sezione 4.4.1](#) ), Così come le visite mirate, corsi di formazione e conferenze. Il nostro obiettivo era quello di garantire che tutto il personale UE coinvolto nel trattamento dei dati personali, a prescindere dalla loro posto nella gerarchia europea, erano a conoscenza delle nuove regole e ciò che essi comportano.



La nostra campagna di sensibilizzazione intensificata nel 2018, al fine di fornire alle istituzioni dell'UE con le conoscenze e gli strumenti necessari per applicare le nuove regole con facilità. La campagna ha messo particolare attenzione l'importanza di [responsabilità](#) , L'idea che le istituzioni dell'UE siano conformi non solo con le nuove regole, ma che sono anche in grado di dimostrare tale conformità. Abbiamo chiesto il top management per impostare il tono, integrando i dati

protezione nei piani di gestione del rischio e garantire che la protezione dei dati è radicata nella cultura della rispettiva istituzione.

Per aiutarli con questo, abbiamo pubblicato aggiornato e nuovi [documenti di orientamento](#) su temi come la responsabilità, la valutazione del rischio e Data Protection di valutazioni d'impatto (DPIAs), le notifiche di violazione dei dati e gli obblighi di trasparenza e di informazione, così come una presa di posizione aggiornato sul ruolo del DPO ( [vedere la sezione 4.4.1](#) ). Questa guida è stata rafforzata attraverso un programma di visite, corsi di formazione e conferenze, tra cui un [visita alle istituzioni e organi in Lussemburgo](#) da garante Wojciech Wiewiórowski, un [sessione di allenamento](#) per il personale presso le agenzie dell'UE ad Atene, uno scambio con

[responsabili della comunicazione delle istituzioni europee](#) e [sessione di allenamento](#) per il personale che lavorano per le agenzie dell'UE, in Italia, oltre a numerosi incontri bilaterali e gli altri con il top management presso le istituzioni europee. ( [vedi figura 2](#) ).

Come istituzione dell'UE, siamo anche soggetti alle nuove regole. Per aiutare a preparare, abbiamo istituito una task force interna sulla transizione al nuovo regolamento. Abbiamo voluto assicurare che fosse in grado di dare il buon esempio e agire come un responsabile [Titolare del trattamento](#) , Fornendo anche assistenza ad altre istituzioni dell'UE.

Non vediamo l'ora di lavorare in stretta collaborazione con le istituzioni europee in questa nuova era di prassi di protezione dei dati, al fine di garantire che continuano a dare l'esempio in materia di protezione dei dati personali in tutta l'UE e nel mondo.

#### 4.1.3-privacy: il completamento del quadro di protezione dei dati dell'UE



Mentre il GDPR regola la protezione dei dati, non si applica per la riservatezza delle comunicazioni. Ulteriore

è richiesta una legislazione, sotto forma di un regolamento sulla privacy, per fornire una protezione completa dei dati all'interno dell'UE e garantire la certezza del diritto e la parità di condizioni per gli operatori del mercato.

L'attuale direttiva e-privacy è stata aggiornata l'ultima volta nel 2009. La proposta di revisione di queste regole è stata presentata dalla Commissione europea il 10 gennaio 2017. Sarebbe sostituire la direttiva con un nuovo [ioni-privacy Regulat](#), all'igning le regole per i servizi di comunicazione elettronica con le norme stabilite nel GDPR.

Secondo le norme vigenti, i fornitori di comunicazioni elettroniche tradizionali sono soggetti a cancellare le limitazioni sul loro modo di utilizzare i dati personali. Le aziende classificate come *servizi della società dell'informazione*, d'altra parte, sono fiorite sfruttando le lacune in questo quadro giuridico. Mentre i fornitori di comunicazioni elettroniche tradizionali devono cercare il consenso per l'utilizzo di dati di comunicazione, servizi della società dell'informazione non sono vincolati agli stessi obblighi. Non v'è, quindi, un bisogno chiaro e urgente di colmare le lacune nella legislazione attuale e rafforzare la tutela della privacy e la sicurezza delle comunicazioni online.

Nel mese di ottobre 2017, il Parlamento europeo ha adottato una risoluzione rapporto e il progetto di regolamento sulla ePrivacy proposto. Abbiamo accolto con favore questo come un tentativo positivo di trovare un equilibrio tra i vari interessi in gioco. Progredire nel Consiglio, tuttavia, è stato più impegnativo.

Il margine di trattativa su molti punti della proposta si limita, in quanto comporterebbe compromettere i principi fondamentali della privacy delle comunicazioni. Ad esempio, quando applicato ai tipi più sensibili di dati personali, clausole che consentono il proposto

*pelliccia elaborazione ther di metadati per finalità compatibili* sarebbe probabilmente ampliare la scappatoia e di servizio presenti fornitori giuridici esistenti con un modo di eludere l'elevato livello di protezione sotto la GDPR.

È fondamentale che il nuovo regolamento e-privacy non abbassa il livello di protezione fornito dal GDPR. Al contrario, data l'importanza di assicurare la riservatezza delle comunicazioni e la particolare sensibilità dei metadati coinvolge, ciò è urgente è la legislazione che fornisce un livello superiore di protezione. Da un punto di vista della protezione dei dati e della privacy, crediamo fermamente che non ci sono scuse per non venire a un accordo sul regolamento ePrivacy prima della fine della legislatura in corso. Non farlo non farà che aumentare il rischio di un esito incerto.



# EDPS Training

## 2 0 1 8



### Brussels - 31 January

We kicked off the year by staying close to home, providing a training course for the European Ombudsman in Brussels (also available to Ombudsman employees in Strasbourg via video link). The course was attended by Heads of Units and Sectors, as well as other relevant staff members.

### Brussels - 16 February (and more)

We staged a two-hour training for EU managers at the European Union School of Administrators (EUSA). This was no one off - we would return to EUSA on six further occasions throughout the year. Thanks to our trainings, EUSA staff are now in a stronger position to negotiate the new Regulation 2018/1725.

### Lisbon - 25 May

On 25 May, we celebrated the entry into force of the GDPR with colleagues from the European Maritime Safety Agency (EMSA) and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) by giving a training event preparing them for the transition to the new Regulation.

### Brussels - 7 June

As summer entered into full swing, we ventured over to Avenue de Beaulieu in Brussels to provide training on new data protection commitments for employees working in DG CLIMA, DG MOVE and other interested colleagues.

### Maastricht - 26 June

On 26th June, and again on 3rd December, the Head of Inspections at the EDPS travelled to Maastricht to give a presentation to participants of EIPA's Data Protection Certification. The two-hour talk was entitled 'supervising data protection compliance: the role of data protection authorities'.

### Luxembourg - 30-31 January

Other EDPS colleagues ventured slightly further afield, providing a two-day training for those working in EU institutions based in Luxembourg. Over 200 guests participated. Whilst there, we delivered a high-level management training session for representatives from the European Parliament, the Commission, CJEU, ECA, EIB, CDT, EIF and CHAFAEA

### Athens - 1-2 March

This two-day training event, provided for staff working at ENISA and CEDEFOP, was a handy opportunity to reaffirm current data protection obligations and introduce the new obligations under the revised Regulation. We also launched a case study on events management which proved so useful that it was re-used at other training sessions throughout the year.

### Brussels - 29 May

Just four days after the General Data Protection Regulation (GDPR) entered into force, the EDPS welcomed 23 recently appointed Data Protection Officers (DPOs) and assistant DPOs from the EU institutions and bodies to a training course on the effective protection of personal data in their new role. A second, similar DPO training event would take place on 10 December.

### Brussels - 14 June

We presented a webinar to the Publications Office of the EU and other EU staff working in publications, communications, social media and web teams. Our work didn't stop there, however. On the same day, we ran a training event for the European Union External Action Service (EEAS).





### Luxembourg - 1-2 October

Invited by the Court of Justice of the EU (CJEU), we returned to Luxembourg to give a training on the new Regulation. Over 400 guests were in attendance, hailing from a number of different EU institutions.

### Stockholm - 18 September

We provided a training session at the annual meeting of the network of web managers from the EU agencies and bodies. It proved a fantastic opportunity to interact directly with EU communication officers on data protection matters.

### Brussels - 7 November

We ran a data protection training event for DG FISMA, the Commission department responsible for EU policy on banking and finance, covering data protection basics, data subject rights and a case study on event management.

### Brussels - 20 November

Just one day before Regulation (EU) 2018/1725 was published, the final training of 2018 was put on for staff of the EFTA Surveillance Authority.

### Paris - 26 November

As we approached the end of the calendar year, the EDPS made a trip to Paris for a Compliance Visit to the European Union Institute for Security Studies. With Assistant Supervisor Wojciech Wiewiórowski also present, the S&E team gave a training on the new Regulation.



### Brussels - 23 October

The European Commission and the national competition authorities in all EU Member States cooperate with each other through the European Competition Network (ECN). In October, we paid DG COMP a visit to guide the ECN on data protection matters in investigations and inspections.

### Turin - 20-21 September

At the request of the European Training Foundation (ETF), we ran through data protection case studies with a wide range of colleagues, including participants from the ETF, the European Food Safety Authority (EFSA), the Joint Research Centre (JRC) and the European University Institute (EUI).

### Frankfurt - 12 November

We were Germany-bound in mid-November to provide a training event on data-protection aspects of banking supervision in cooperation with the Data Protection Officer of the European Central Bank (ECB), the private sector (Union Investment) for ECB staff, and staff of the European Insurance and Occupational Pensions Authority (EIOPA) in Frankfurt.

### Brussels - 21 November

21st November saw the EDPS give a presentation to the Committee for Civil Aviation Security at DG MOVE.

### Brussels - 3 December

The EDPS ended the year's training sessions in the same place in which we started, at home in Brussels. We provided training to DG COMM and other European Commission representations on how the new Regulation would affect their events.

Figura 2. programma di formazione GEPD 2018



#### 4.1.4 Privacy by Design: la tecnologia che serve il popolo

Il dibattito pubblico sul cattivo uso dei dati personali per il monitoraggio e la finalità di profilazione e il ruolo della tecnologia nella nostra società è intensificata nel corso del

2018. Un elemento del dibattito è se le aziende dovrebbero essere in grado di sfruttare la tecnologia esclusivamente come un mezzo per aumentare i profitti, o se essi dovrebbero anche essere obbligati a usarlo per favorire gli interessi dei singoli e del bene comune.

Il GDPR ha introdotto i principi di protezione dei dati in base alla progettazione e per impostazione predefinita gli obblighi essenziali per garantire la responsabilità. I responsabili per la raccolta e il trattamento dei dati personali deve mettere in atto adeguati metodi tecniche e organizzative per garantire e dimostrare la conformità alla protezione dei dati. Entrambi i principi hanno il potenziale per contribuire a stabilire il punto di vista umano come il driver principale per lo sviluppo tecnologico. La protezione dei dati in base alla progettazione comporta la pianificazione per l'integrazione della protezione dei dati personali in nuovi sistemi tecnologici e processi dalla fase di progettazione di un progetto e in tutto il ciclo di vita, mentre la protezione dei dati di default prevede l'integrazione di tutela della privacy in tutti i servizi tecnologici e prodotti come un default ambientazione.

Il 31 maggio 2018, pochi giorni dopo la GDPR divenuto pienamente applicabile, abbiamo pubblicato un [Parere preliminare sulla Privacy by Design](#). Il parere mirava a costruire il nostro lavoro con la [Internet Privacy rete Ingegneria \(IPEN\)](#) (vedere la sezione 4.4.16) e sulla [GEPD Ethics Initiative](#) (vedere paragrafo 4.6), Per favorire il dialogo tra i responsabili politici, le autorità di regolamentazione, industria, mondo accademico e della società civile su come le nuove tecnologie possono essere progettati a beneficio dell'individuo e della società. Ci auguriamo di poter ulteriormente il dibattito su questo tema nei nostri tentativi di stabilire un approccio comune allo sviluppo tecnologico, che mette al primo posto la dignità umana.

## 4.2 EUROPOL SOVRINTENDERE

Europol è l'organismo dell'UE responsabile del sostegno le autorità di contrasto degli Stati membri nella lotta contro la criminalità internazionale e il terrorismo gravi. Il 1 ° maggio 2017, il GEPD ha assunto la responsabilità di vigilare sul trattamento dei dati personali presso l'Europol.

Il [regolamento Europol](#) compiti al GEPD vigilare sul trattamento dei dati personali relativi alle attività operative di Europol s'. Siamo inoltre responsabile della supervisione del trattamento dei dati personali relativi alle attività amministrative di Europol, compresi i dati personali relativi al personale di Europol. Tuttavia, questo compito di vigilanza è soggetta alle norme contenute nella nuova [regolamento 2018/1725](#), Che sostituisce [regolamento 45/2001](#).

Una delle principali sfide che dobbiamo affrontare in questo ruolo è quello di garantire che l'Europol il giusto equilibrio tra sicurezza e la privacy quando si tratta di trattamento dei dati a fini di applicazione della legge. Un'Europa sicura e aperto richiede una maggiore efficacia operativa nella lotta contro la criminalità transfrontaliera, ma richiede anche un impegno per la tutela dei diritti e delle libertà fondamentali degli individui.

### 4.2.1 cooperazione continua con l'unità di protezione dei dati dell'Europol

Ai sensi del regolamento di Europol, Europol deve nominare un [Protezione dei dati ICER f \(DPO\)](#), che deve agire in modo indipendente le prestazioni di tutti compiti. Attraverso la stretta collaborazione con i DPO di Europol e l'unità Funzione di protezione dei dati (DPF), siamo meglio attrezzati per monitorare il rispetto di Europol con il regolamento e di fornire consulenza alla squadra DPF quando ne hanno bisogno.

Il nostro obiettivo è di facilitare e rafforzare la nostra cooperazione organizzando riunioni regolari con il DPF e altro personale operativo pertinente. Questi incontri, che di solito si svolgono su base bimestrale, sono l'occasione per discutere di eventuali nuovi progetti o procedure di elaborazione dati di previsione da Europol, così come altre questioni in sospeso.

Nel corso dell'ultimo anno, il GEPD e il DPF si sono incontrati quattro volte a L'Aia, l'8 febbraio, 24 aprile, 9 luglio e 16 ottobre 2018. Abbiamo anche incontrato con il DPF e gli altri membri del personale dell'Europol a Bruxelles il 25 Settembre 2018. questi incontri ci aiutano per anticipare le questioni specifiche relative alle attività di trattamento dei dati presso l'Europol e di definire e pianificare le attività future, come le ispezioni o richieste di informazioni. Tre membri del personale del GEPD hanno partecipato anche nei dati europea

Gli esperti di protezione di rete (EDEN) conferenza, che ha avuto luogo il 22-23 novembre 2018 ( [vedere la sezione 4.2.7](#) ).



#### 4.2.2 Supervisione progetti analisi operativa

Regolamento Europol permette l'elaborazione dei dati per supportare ciò che è noto come analisi operativa. Tuttavia, si precisa che tali indagini e operazioni di intelligence criminale, che vengono effettuati dalle autorità di contrasto degli Stati membri, devono essere eseguiti come parte di un progetto di analisi operativa.

Ogni progetto di analisi operativa si riferisce ad un particolare tipo di reato, come la pornografia infantile, la criminalità informatica, il traffico di droga, i gruppi criminali organizzati, reati contro il patrimonio o il terrorismo. Per ogni progetto, l'Europol è tenuto a definire e comunicare il GEPD su:

- lo scopo specifico del progetto;
- le categorie di dati coinvolti e le persone si tratta;
- i partecipanti, che potrebbero essere gli Stati membri, paesi o organizzazioni non-UE;
- la lunghezza di tempo in cui i dati vengono memorizzati;
- le condizioni di accesso ai dati in questione e per qualsiasi proposta di trasferimento di tali dati.

Alla fine del 2018, l'Europol aveva un portafoglio di 30 progetti di analisi operativa. Non abbiamo ricevuto notifica formale di eventuali nuovi progetti nel 2018, anche se c'è stato notificato di piccole modifiche a progetti esistenti e stati consultati sulle modifiche previste prima della modifica reale del portafoglio. Tutti i progetti di analisi sono elencati e descritti sulla [sito Europol](#) .

#### 4.2.3 Ispezione Europol

L'8 maggio 2018, abbiamo pubblicato un rapporto sulla nostra prima ispezione dell'Europol, effettuata nel dicembre 2017. Come con i nostri altri controlli ( [vedere la sezione 4.4.6](#) ), I risultati non sono stati condivisi pubblicamente, ma il rapporto è stato condiviso con la nazionale [autorità per la protezione dei dati](#) (DPA) attraverso il segretariato del consiglio di cooperazione Europol ( [vedere la sezione 4.2.6](#) ). Abbiamo delineato una serie di raccomandazioni per il miglioramento e noi continueremo a lavorare con l'Europol per garantire che hanno messo le nostre raccomandazioni in pratica.

Abbiamo effettuato una seconda ispezione dal 22-25 Maggio 2018. Tre esperti dei DPA di Francia, Grecia e Italia unite l'ispezione come parte del team GEPD. Gli Stati membri sono i principali fornitori di informazioni di Europol giù di lì, così come beneficiando di loro competenza, la partecipazione di esperti nazionali nel processo di ispezione contribuisce ad aumentare la consapevolezza dei problemi derivanti a livello di Europol che potrebbero aver avuto origine a livello nazionale. Questo potrebbe includere problemi relativi alla qualità dei dati o giustificazione insufficiente per il trattamento di dati sensibili, per esempio. Essi possono quindi prendere in considerazione come affrontare questi problemi nella loro attività di vigilanza a livello nazionale.

La parte legale del controllo si è concentrato su quattro temi, i primi due dei quali erano particolarmente alto profilo:

##### 1. Il trattamento dei dati nell'ambito del progetto analisi operativa dell'Europol, *I viaggiatori*: Ciò riguarda i dati

personali di persone che viaggiano da e verso zone di conflitto, la Siria in particolare. Essa comprende quelli noti come combattenti terroristiche straniere e delle loro famiglie, compresi i bambini.

##### 2. Il trattamento dei dati sui migranti che arrivano a hotspot in Grecia e in Italia: L'Agenzia europea delle frontiere e della guardia

costiera (Frontex) interviste migranti al loro arrivo in questi paesi. Se si crede a un individuo di presentare un possibile rischio per la sicurezza, gli Stati membri possono rivolgersi a Europol *agenti distaccati*,

anche situato nelle hotspot, per eseguire controlli su di essi.

##### 3. Il trattamento dei dati relativi a persone di 18 anni in tutti i progetti di analisi operativa, in particolare nei casi in cui tali individui sono etichettati come sospetti: Ai sensi del

regolamento Europol, l'Europol è consentito solo al trattamento dei dati personali dei minori di 18 anni se così facendo è strettamente necessario e proporzionato allo scopo di prevenire o combattere il crimine sotto il mandato di Europol.

##### 4. Il trattamento dei dati nel Europol

**Sistema informativo:** Questo è il database di Europol di

indagati, condannati e potenziali criminali futuri. In particolare, ci siamo concentrati su come questo database viene aggiornato da parte degli Stati membri ed Europol per conto di paesi terzi.

L'elemento tecnico dell'ispezione cercato di costruire sulle attività svolte come parte del nostro primo sopralluogo. Ci siamo concentrati su tre aree in particolare:

1. Le procedure di gestione della sicurezza delle informazioni di Europol;

gestione dei log 2. utente;

3. il processo di validazione di nuovi strumenti e sistemi informatici.

Abbiamo pubblicato il nostro rapporto di ispezione, il 19 dicembre 2018. Ci sarà il follow-up con Europol sulle nostre raccomandazioni ic specif durante tutto l'anno a venire.

Nel 2018, abbiamo anche effettuato controlli a distanza di due siti web Europol come parte del nostro esercizio di follow-up in materia di protezione dei dati personali trattati da siti web delle istituzioni UE ( [vedere la sezione 4.4.7](#) ).

#### 4.2.4 Consulenza Europol

Il GEPD raccomanda Europol su tutte le questioni relative alla protezione dei dati, sia di nostra iniziativa o in risposta ad una consultazione.

##### consultazioni preliminari

Europol deve presentare una richiesta preventiva consultazione al GEPD per ogni nuova attività di trattamento dei dati che prevede di effettuare che comporta il trattamento di dati sensibili o che potrebbero presentare un rischio specifico per gli individui. Sulla base di presentazione di Europol, analizziamo in che misura l'operazione di trattamento proposto è conforme al regolamento Europol e tutti gli altri principi e le regole di protezione dei dati rilevanti. Abbiamo quindi a disposizione di Europol con raccomandazioni che devono mettere in atto per garantire la conformità.

Nel 2018, abbiamo pubblicato tre pareri. Questi tutti relativi a consultazioni preliminari pervenuta alla fine del 2017. I Commenti interessati i seguenti strumenti tecnici:

- **QUEST (Interrogazione di Europol Systems):** Un'interfaccia automatica utilizzato per facilitare **controllo incrociato** dei dati nelle banche dati nazionali e database sospetto di Europol. Attraverso il suo meccanismo di ricerca semplificata, Quest fornisce agli Stati membri con nuove funzionalità di ricerca. In questo modo gli ufficiali autorizzati di polizia degli Stati membri di effettuare ricerche simultanee del sistema di informazione Europol e altre banche dati nazionali e internazionali dal proprio

ambienti di lavoro, utilizzando le loro banche dati nazionali.

- **ETS (soluzione europea di inseguimento):** Uno strumento che permette di unità specializzate, con sede prevalentemente negli Stati membri, di scambiare dati di geo-localizzazione in tempo quasi reale. E 'usato per tracciare e rintracciare gli oggetti e gli individui.
- **Irma (Internet applicazione Referral Management):** Uno strumento software utilizzato dall'Unità Referral interna di Europol (**IRU**) per automatizzare il **processo di riferimento**, il **processo di identificazione** contenuti terroristici on-line e la notifica fornitori di servizi online della necessità di rimuoverlo. Europol ha sviluppato questo strumento e vorrebbe fornire agli Stati membri, da utilizzare per lo stesso scopo.

Dato che questi pareri si riferiscono all'utilizzo di strumenti da parte delle autorità di contrasto nazionali, che possono comportare supervisione da parte delle rispettive autorità di vigilanza nazionali, il GEPD hanno condiviso i pareri con loro.

Nel 2018, abbiamo ricevuto una preventiva consultazione supplementare su SIENA 4.0, la versione aggiornata del sistema di scambio di messaggio sicuro di Europol. Viene utilizzato per gestire lo scambio di informazioni operative e strategiche reati legati tra gli Stati membri, Europol e altri partner di Europol. Pubblicheremo feedback su questa consultazione preventiva nel 2019.

##### Consultazioni e indagini

Abbiamo pubblicato una guida e condotto indagini di propria iniziativa su una serie di questioni nel 2018. Uno di questi casi è stata una consultazione relativo al Internet Corporation for Assigned Names e Numbers (ICANN). **Nostro Opinione indirizzata se Europol dovrebbe** agire come organismo di accreditamento per le forze dell'ordine (LEA) che cercano di accedere ai dati personali nel database WHOIS, di Internet Domain Name System che è gestito da ICANN.

Prima di **Il regolamento generale sulla protezione dei dati (GDPR)** è entrata in vigore il 25 maggio 2018, i dati personali di tutti coloro registrazione di un nuovo nome di dominio è stato pubblicamente visualizzati su internet, attraverso il servizio WHOIS. Ciò ha incluso nomi, indirizzi email, numeri di telefono e altre forme di informazioni di identificazione.

Tuttavia, al fine di rispettare i requisiti della GDPR, queste informazioni in precedenza pubblica viene ora redatta. Questo ha creato problemi per i LEA, che non hanno più come ad un facile accesso ai dati personali dei nomi di dominio dichiaranti, e sono ora tenuti a concludere le procedure giuridiche formali per poter accedere alle informazioni rilevanti.

Il nostro parere ha concluso che l'Europol potrebbe fungere da *accreditor forze dell'ordine*. Ciò comporterebbe che fornisce garanzie ai registri e registrar che ogni LEA UE che cercano di accedere ai record WHOIS è davvero un'autorità legittima, a condizione che l'attività in questione rientra nel mandato di Europol, come autorità di supporto per gli Stati membri.

In un caso separato, abbiamo fornito indicazioni sul trasferimento dei dati personali da Guardia Border Agency e costa europea (Frontex) per l'Europol. Frontex è coinvolto nel monitoraggio dei flussi migratori e la realizzazione di analisi dei rischi in materia di gestione integrata delle frontiere, compresa la sicurezza interna o la sicurezza alle frontiere esterne dell'UE. La nostra guida concerne i trasferimenti di dati da Frontex di Europol in relazione a tali attività.

In aggiunta a questo, abbiamo condotto un'indagine su dati elaborati nel contesto della 'Crime Information cellulare' (CIC), un progetto pilota attivato sul quadro operativo EUNAVFOR MED *Sophia*, operanti nel Mar Mediterraneo centrale. A seguito di una decisione del Consiglio dell'UE del 14 giugno 2018, di personale specializzato da Europol e Frontex hanno intrapreso a bordo Flagship EUNAVFOR MED. L'obiettivo è quello di migliorare lo scambio di informazioni tra la sicurezza comune e la politica di difesa (PESD) e la giustizia e gli affari interni (GAI) attori in attività criminali nel Mediterraneo centrale e smantellare le reti criminali nella zona, in particolare coloro che sono coinvolti nel traffico di migranti e traffico di esseri umani.

Abbiamo anche consigliato Europol sui possibili sviluppi in materia di FIU.net. Questa è la rete di informazione decentrato che supporta Intelligence Units finanziario dell'UE (FIU) nella loro lotta contro il riciclaggio di denaro e la f INANZIAMENTO del terrorismo. E 'gestito da Europol.



#### 4.2.5 vengono trattati i reclami

Il GEPD è anche responsabile per l'udito e l'esame delle denunce da parte di persone che credono che

Europol ha gestito male i propri dati personali. Europol si basa su autorità di contrasto nazionali per fornire loro la maggior parte dei dati personali che elabora. Come queste autorità nazionali sono supervisionate da loro DPA nazionali, lavoriamo in consultazione con le pertinenti DPA nazionali per indagare su tutte le denunce ricevibili e adottare le decisioni.

Dei due reclami ricevuti nel 2017, solo uno è stato considerato ammissibile. E 'legato ad un'affermazione che l'Europol negato l'accesso ai dati personali richiesti dal diretto interessato. Abbiamo studiato la denuncia, esaminando il file di Europol sulla decisione e tenendo conto delle osservazioni del DPA nazionali coinvolti. La nostra conclusione, rilasciato nel 2018, è stata che la decisione dell'Europol di rifiutare l'accesso ai dati personali è lecito in questo caso.

Nel 2018, abbiamo ricevuto una sola denuncia, che è stato considerato irricevibile.

#### 4.2.6 Incontro con il Consiglio di cooperazione

Proprio come il GEPD ha il compito di vigilare sul trattamento dei dati personali da parte di Europol, le DPA nazionali sono responsabili della supervisione del trattamento dei dati personali da parte delle rispettive autorità di contrasto nazionali. Come la maggior parte dei dati trattati da Europol viene da parte delle autorità di contrasto nazionali, è indispensabile che siamo in grado di cooperare efficacemente con le DPA nazionali.

Oltre ad attività quali supervisione congiunta, gran parte di questa cooperazione si svolge in riunioni del Consiglio di cooperazione, per il quale il GEPD fornisce la segreteria. Il Consiglio ha una funzione di consulenza e fornisce un forum per discutere di problemi comuni e sviluppare linee guida e buone pratiche.

Composto da rappresentanti delle DPA nazionali e il GEPD, il Consiglio si riunisce almeno due volte l'anno. Nel 2018, questi incontri hanno avuto luogo il 30 maggio e il 3 ottobre.

Il primo incontro ha fornito l'occasione per noi di condividere informazioni sulle attività di vigilanza che avevano avuto luogo dal momento che il nostro precedente incontro del 16 novembre 2017. Ciò ha incluso il nostro primo sopralluogo Europol. E 'stato anche l'occasione per discutere il programma di lavoro del Consiglio per i prossimi due anni.

Garante Wojciech Wiewiórowski aperto il nostro secondo incontro. Nel suo discorso ha sottolineato che la fruttuosa cooperazione tra il GEPD e DPA dipende dalla fiducia e reciprocità. Solo in un tale ambiente il Consiglio può avere successo nella protezione dei diritti dei cittadini.

Abbiamo poi concentrati sulle attività di Europol che hanno un effetto a livello nazionale. Ad esempio, l'Europol fornisce gli strumenti che facilitano lo scambio di informazioni tra le autorità di contrasto nazionali e le DPA nazionali sono responsabili della supervisione il loro uso a livello nazionale. A questo proposito, le discussioni hanno avuto luogo l'uso di ETS da parte delle autorità di contrasto nazionali e sui possibili sviluppi di FIU.net ( [vedere la sezione 4.2.4](#) ).

Un aggiornamento di un volantino volto ad aiutare le persone a esercitare i diritti di protezione dei dati in relazione a Europol e un manuale per le autorità di contrasto nazionali su come inviare i dati a Europol sono stati anche discussi.

Ci auguriamo di poter rafforzare la nostra collaborazione con il consiglio mentre lavoriamo verso il raggiungimento del comune obiettivo di un'Europa sicura e aperta.

#### 4.2.7 Impostazione del tono a livello di gestione

L'8 marzo 2018, Caterina De Bolle, ex commissario generale della polizia federale belga, è stato nominato il nuovo direttore esecutivo di Europol. Accompagnato dal Europol DPO e da due membri del suo gabinetto, ha visitato il GEPD il 16 luglio 2018 per incontrare i GEPD Giovanni Buttarelli. Questo incontro è stato un'ottima occasione per entrambe le parti di conoscersi l'un l'altro e stabilire le basi per una cooperazione efficace, basato sulla fiducia reciproca.

Il loro scambio di opinioni era sia franco e costruttivo. Il nuovo direttore esecutivo ha mostrato una buona comprensione delle questioni relative alla protezione dei dati in generale e uno ancora migliore conoscenza dei problemi principali che l'Europol e il GEPD devono ancora affrontare. Gestione dà il tono per la cooperazione in tutta l'intera organizzazione, quindi non vediamo l'ora di proseguire la cooperazione e costruttivo a questo livello nel corso dei prossimi mesi e anni.

Nello spirito di guidare con l'esempio attraverso la cooperazione efficace, il 22 novembre 2018, garante Wojciech Wiewiórowski ha dato il discorso ad una conferenza sulla libertà e la sicurezza, organizzato congiuntamente dalla Europol dati esperti di protezione della rete (EDEN) e l'Accademia di diritto europeo (ERA). Ha ricordato il messaggio delineata dall'ex direttore dell'Europol esecutivo Rob Wainwright nella sua [Giornata della protezione dei dati 2018 post sul blog](#) , Chiedendo norme di protezione dei dati su misura per l'applicazione della legge. Ha inoltre sottolineato che una maggiore sicurezza può essere raggiunto senza limitare i diritti di protezione dei dati. Attraverso la loro continua

e costruttiva collaborazione, il GEPD e l'Europol sono nella posizione ideale per dimostrare questo.



#### 4.2.8 Il Joint esame parlamentare Gruppo

L'esame parlamentare gruppo misto (JPSG) è un organo parlamentare di vigilanza composto da più di 120 rappresentanti del Parlamento europeo e dei parlamenti nazionali. Il suo compito è quello di tenere Europol responsabile delle sue attività. Il GEPD devono supportare il JPSG in questo ruolo.

Almeno una volta l'anno, il JPSG organizza un incontro con il GEPD per discutere il rispetto Europol delle norme sulla protezione dei dati e principi. Nel 2018, due riunioni del JPSG hanno avuto luogo e il GEPD è stato invitato a partecipare a entrambi. Questi hanno avuto luogo a Sofia, Bulgaria il 19 marzo 2018 e a Bruxelles il 25 settembre, 2018.

Gli incontri sono un'opportunità per noi di fornire la JPSG con una panoramica delle attività di vigilanza del GEPD, nonché per discutere questioni più specifiche. Nel corso della riunione di Sofia, ad esempio, abbiamo affrontato una serie di raccomandazioni relative allo scambio di dati personali tra Europol e otto diversi paesi mediorientali e africani. Queste raccomandazioni sono state emesse dalla Commissione nel dicembre 2017 e consigliato il Consiglio dell'Unione europea di avviare i negoziati per gli accordi internazionali con gli otto **paesi sullo scambio di dati**. Il GEPD ha pubblicato un [Opinione](#) su queste raccomandazioni poco prima della riunione JPSG il 14 marzo 2018 ( [vedere la sezione 4.3.4](#) ).

## GEPD supervisione di Europol nel 2018:

### le statistiche



Al secondo incontro, ci siamo concentrati in particolare sulla dipendenza di Europol sulla cooperazione per svolgere il suo ruolo, le implicazioni di questo per questioni di protezione dei dati e su come stiamo lavorando con l'Europol per affrontare tali implicazioni. partner di Europol sono molteplici, tra cui i partner internazionali, i partner dell'UE quali Frontex e partner a livello nazionale.

Siamo ansiosi di cooperare ulteriormente con la JPSG nel corso del 2019.

### 4.3 SICUREZZA E FRONTIERE UE

Come abbiamo stabilito nel [strategia GEPD](#), Ci siamo impegnati a facilitare la definizione delle politiche responsabile e consapevole all'interno dell'UE e alla promozione di una conversazione matura sulla sicurezza e la privacy come parte dei nostri sforzi per aprire un nuovo capitolo nella protezione dei dati nell'UE.

Negli ultimi anni, il legislatore europeo ha presentato una vasta gamma di proposte politiche volte ad accrescere la sicurezza dell'UE e il miglioramento della gestione delle frontiere. Terrorist a chiodini, la crisi migrazione e lo sviluppo di tecnologie sempre più sofisticate sono i principali fattori alla base di queste proposte, tutte

che mirano ad assicurare che i processi e le politiche dell'UE rimangono all'altezza del compito di assicurare sicuro e sicuro confini dell'UE.

Sosteniamo pienamente questi sforzi e riconosciamo la necessità urgente per la politica europea di adattarsi alle nuove realtà. Tuttavia, una maggiore sicurezza non deve andare a scapito dei diritti fondamentali garantiti dalla [Carta UE](#).

In linea con gli impegni individuati nella nostra strategia, cerchiamo di fornire al legislatore con adeguata consulenza legale, orientamento e raccomandazioni per garantire che i politici siano in grado di prendere decisioni informate in materia di politica delle frontiere dell'UE. Inoltre, ci proponiamo di sostenere il legislatore lavorando in stretta collaborazione con i nostri simili [autorità dell'UE sulla protezione dei dati \(DPA\)](#) per garantire che gli strumenti utilizzati per attuare la politica delle frontiere dell'UE continuano a funzionare secondo i più alti standard in materia di protezione dei dati dell'UE.

#### 4.3.1 Il controllo efficace dei sistemi IT su larga scala

L'Unione europea gestisce diversi [su larga scala database IT](#). Questi sono utilizzati per sostenere le politiche dell'UE in materia di asilo, gestione delle frontiere, la cooperazione di polizia e

migrazione. Attraverso le banche dati, le autorità nazionali, così come alcuni organi dell'UE, sono in grado di scambiare informazioni relative ai confini, la migrazione, i costumi e le indagini della polizia.

Il GEPD è responsabile della supervisione del trattamento dei dati personali nelle unità centrali delle banche dati, la maggior parte dei quali sono ospitati dall'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nel settore della libertà, sicurezza e giustizia (eu-Lisa). Le DPA nazionali sono responsabili della supervisione come le autorità nazionali utilizzano questi sistemi. La divisione dei compiti tra DPA dell'UE e il GEPD rispecchia la suddivisione dei compiti tra l'unità centrale di gestione del sistema e le autorità nazionali che lo utilizzano. L'autorità di vigilanza competente dipende quindi che elabora i dati.

Una delle nostre responsabilità di supervisione è di effettuare ispezioni periodiche delle banche dati centrali. Tali ispezioni si concentrano sulla sicurezza e la gestione dei sistemi, mentre le autorità nazionali sono tenuti a garantire l'accuratezza delle informazioni inserite in loro. Attraverso le ispezioni, siamo in grado di controllare il rispetto della protezione dei dati, ma anche di lavorare **direttamente con eu-LISA per migliorare responsabilità nella gestione** di questi database.

Nel 2018, abbiamo effettuato ispezioni in loco della **Sistema d'informazione Schengen (SIS)** e la **Sistema d'informazione visti (VIS)**. Condivideremo la nostra relazione e le raccomandazioni con eu-LISA, al Parlamento europeo, al Consiglio, alla Commissione europea, e DPA nazionali nel 2019 e seguire con loro di conseguenza.

#### 4.3.2 controllo coordinato di sistemi IT su larga scala

Proprio come il GEPD è responsabile della supervisione delle unità centrali di basi di dati su larga scala dell'UE, le DPA nazionali sono responsabili della supervisione come le loro rispettive autorità nazionali utilizzano questi database. Per assicurare la coerenza degli sforzi di supervisione su entrambi i livelli, tutte le autorità interessate, compreso **il GEPD, cooperano attraverso Supervisione gruppi di coordinamento (SCGS)**. Ognuno di questi gruppi è dedicato a un database specifico UE.

Costituito da rappresentanti delle DPA nazionali e il GEPD, i SCGS si incontrano regolarmente per garantire coordinata supervisione end-to-end di tutti i database. Come l'autorità di vigilanza per le unità centrali, il GEPD partecipa come membro a pieno titolo di questi gruppi. Forniamo anche la segreteria del

gruppi, operante sotto l'autorità dei rispettivi presidenti.

Come negli anni passati, i gruppi si sono incontrati due volte nel 2018. I SCGS per **Eurodac**, **SIS** e **VIS** sono incontrati a giugno e novembre, mentre lo SCG per la **Sistema d'informazione doganale (CIS)** si è riunito in maggio e ottobre. I risultati di questi incontri sono **pubblicati sul loro rispettive pagine web sul sito web del GEPD**. Gli incontri continuano a fornire un forum importante per la cooperazione tra lo Stato membro DPA e il GEPD, pur rispettando il ruolo e le competenze di ciascuno.

Le nuove regole sulla protezione dei dati per le istituzioni e gli organi dell'UE prevedono un unico modello di controllo coordinato di entrambi i sistemi IT su larga scala e le agenzie e organi dell'Unione, all'interno del Consiglio europeo per la protezione dei dati (EDPB). L'EDPB ha quindi lanciato un'iniziativa per riflettere su come organizzare questo controllo coordinato nel quadro EDPB.

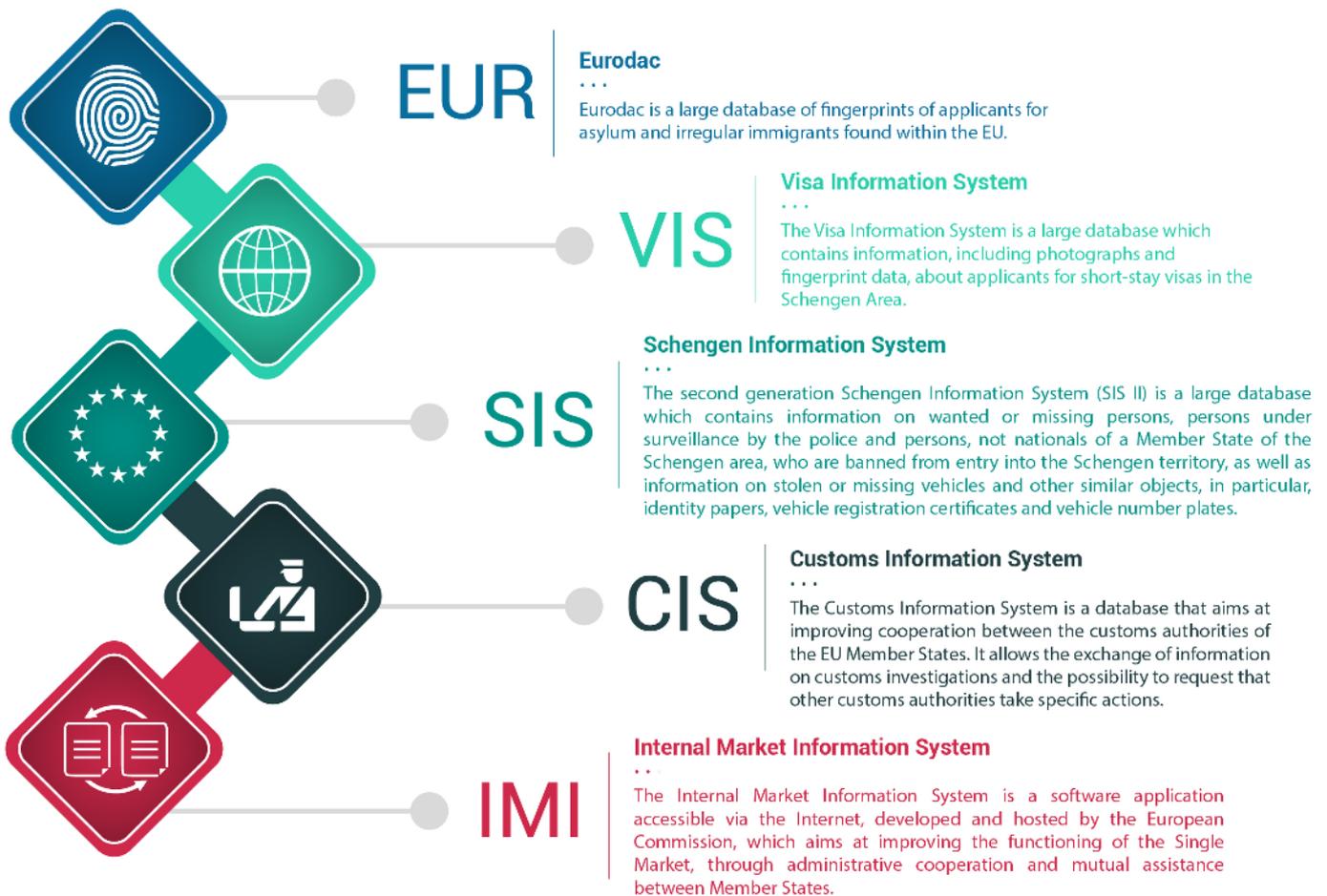
I SCGS si incontreranno di nuovo nel 2019 come parte del nostro continuo impegno per garantire un controllo efficace, efficiente, coordinato e coerente di queste banche dati importanti.

#### 4.3.3 Observing Schengen

La creazione dello spazio Schengen ha fatto un viaggio tra i molti paesi dell'UE un'esperienza molto più facile e più divertente per i cittadini dell'UE e altri. Tuttavia, il successo di questa iniziativa dipende da uno sforzo di collaborazione da tutti gli Stati coinvolti.

Tra le misure volte a garantire che tutti gli Stati membri interessati in modo adeguato implementare regole di Schengen sono **regolari esercizi di revisione tra pari**. Conosciuto come **valutazioni Schengen** (valutazione di Schengen), dette valutazioni paritarie sono organizzati dalla Commissione europea e realizzato da esperti degli Stati membri. Il GEPD spesso partecipa come osservatore nella parte protezione dei dati della valutazione.

Con la nostra esperienza supervisione delle unità centrali del SIS e VIS (**vedere la sezione 4.3.1**), il GEPD è in grado di offrire una prospettiva differente e complementare sul processo di valutazione di Schengen. Questo è un chiaro valore aggiunto nella supervisione, l'applicazione e la promozione della protezione dei dati in questo settore altamente sensibile. Il nostro ingresso è apprezzato anche sul piano linguistico, come la composizione internazionale della nostra istituzione significa che i membri del personale del GEPD che prendono parte alla valutazione spesso parlano la lingua del paese in fase di valutazione.



L'aspetto della protezione dei dati della valutazione coinvolge valutare la conformità delle autorità competenti delle norme sulla protezione dei dati, tra cui la sicurezza del SIS e VIS anche dati; il ruolo e poteri dell'autorità di protezione dei dati nazionali; la consapevolezza del pubblico di Schengen; e la cooperazione internazionale. Nel corso di un anno, di solito prendere parte a tre SCHEVALs. Nel 2018 abbiamo agito in qualità di osservatore per le valutazioni della Svizzera, Lettonia e Finlandia.

#### 4.3.4 Tutela dei diritti fondamentali nel settore della libertà, sicurezza e giustizia

carte d'identità biometriche

Il 10 agosto 2018, abbiamo emesso un [Opinione](#) sulla proposta della Commissione di un regolamento volto a rafforzare la sicurezza delle carte d'identità e altri documenti rilasciati ai cittadini dell'UE e le loro famiglie. Ciò comporterebbe il miglioramento delle caratteristiche di sicurezza delle carte d'identità dei cittadini dell'Unione europea e le carte di soggiorno dei familiari extracomunitari.



@EU\_EDPS

# GEPD ribadisce l'importanza di # protezione dati principi chiave quando rafforzamento della sicurezza delle carte d'identità dei cittadini dell'UE. #Necessità & # Proporzionalità devono essere rispettati quando i dati vengono elaborati, soprattutto # biometrico dati @EP\_Justice [http:// europa.eu/Gf93pT](http://europa.eu/Gf93pT)

La proposta avrebbe un impatto su un massimo di 370 milioni di cittadini dell'Unione europea, potenzialmente sottoponendo l'85% della popolazione dell'UE alle esigenze impronte digitali obbligatorie. Tenendo conto di questa ampia portata e sensibile

la natura dei dati coinvolti, abbiamo individuato la necessità vitale per la Commissione di dimostrare chiaramente la necessità delle misure proposte. Ad esempio, gli scopi dichiarati per la lavorazione di due tipi distinti di dati biometrici, ovvero immagini facciali e impronte digitali, potrebbe essere realizzato utilizzando un approccio meno invasivo, e quindi non riescono a dimostrare necessità. Abbiamo anche citato la necessità di stabilire garanzie esplicite per assicurare che l'attuazione della proposta a livello nazionale non porterebbe alla creazione di banche dati nazionali di impronte digitali.

Mentre la memorizzazione di immagini di impronte digitali fa migliorare l'interoperabilità (vedere la sezione 4.3.4), Aumenta anche la quantità di dati biometrici che viene elaborato. Questo aumenta il rischio di rappresentazione in caso di una violazione dei dati personali. Di conseguenza, è consigliabile limitare notevolmente i dati relativi alle impronte digitali memorizzati nel chip di documenti di soggiorno, per includere solo un sottoinsieme delle caratteristiche estratte dall'immagine digitale.

Infine, il GEPD ha sostenuto l'impostazione del limite minimo di età per la raccolta delle impronte digitali dei bambini per 14 anni, in linea con l'approccio adottato in altri strumenti del diritto dell'UE.



 @EU\_EDPS

**#GEPD** chiede un più ampio dibattito sul futuro della condivisione delle informazioni in **#UNIONE EUROPEA** .

Leggi il parere del GEPD sulla **#interoperabilità** tra i sistemi informativi su scala dell'UE larga [http:// europa. eu /! Rv88rR](http://europa.eu/Rv88rR) e il comunicato [http:// europa.eu/uW44UM](http://europa.eu/uW44UM)

Più ampio dibattito necessario sul futuro della condivisione delle informazioni nell'UE

Al fine di affrontare le sfide relative alla sicurezza e gestione delle frontiere, l'UE deve adottare un approccio più intelligente per la condivisione delle informazioni. Interoperabilità potrebbe rivelarsi uno strumento utile, ma è anche probabile che avere conseguenze legali e sociali profonde, come indicato nel nostro

[documento di riflessione](#) sul tema nel novembre 2017.

Su 16 Apr 2018 abbiamo seguito il nostro documento di riflessione con una **Opinione** sulle proposte di due regolamenti che creano un quadro per l'interoperabilità tra i sistemi di informazione su larga scala UE.

L'interoperabilità è il processo che consente queste grandi banche dati dell'UE per comunicare e scambiare informazioni. Potrebbe aiutare le autorità pubbliche a gestire le questioni relative alla migrazione, asilo e sicurezza, facilitando lo scambio di dati raccolti all'interno dei database.

Le proposte prevedono la possibilità di utilizzare i sistemi più estesamente, oltre gli obiettivi specifici per cui sono stati stabiliti. In particolare, i dati memorizzati nei diversi sistemi sarebbero riuniti al fine di combattere le frodi di identità, ma anche per facilitare e consentire controlli di identità nel territorio dello Stato membro. Avrebbero anche semplificare l'accesso delle forze dell'ordine ai database che non contengono informazioni di polizia. Di particolare interesse è la creazione di una banca dati contenente informazioni centralizzate di milioni di cittadini non comunitari, compresi i dati biometrici. La scala del database e la natura dei dati da memorizzare al suo interno significa che una violazione dei dati potrebbe danneggiare un numero molto elevato di persone.

Mentre le autorità di contrasto hanno bisogno di accedere ai migliori strumenti possibili per combattere il terrorismo e altri reati gravi, consentendo alle autorità di contrasto di accedere regolarmente informazioni non originariamente raccolte per finalità di contrasto ha implicazioni significative per la tutela dei diritti fondamentali. E 'quindi essenziale che misure di salvaguardia severe e adeguate legali, tecniche e organizzative sono costruiti per tutti i database comunitari, e che particolare attenzione è data a definire le funzioni e condizioni di utilizzo.

Date le implicazioni incerte di questa proposta per la protezione dei dati e di altri diritti fondamentali e delle libertà, abbiamo chiamato per un più ampio dibattito sulla questione prima di prendere ulteriori passi verso l'attuazione.



## Lo scambio di informazioni tra l'Europol e paesi terzi nella lotta contro il terrorismo e la criminalità

La Commissione europea ha adottato otto raccomandazioni, il 20 dicembre 2017. In queste raccomandazioni, hanno chiesto al Consiglio dell'Unione europea l'autorizzazione ad avviare i negoziati con l'Algeria, l'Egitto, Israele, Giordania, Libano, Marocco, Tunisia e Turchia di concludere accordi internazionali sullo scambio di dati tra Europol e questi otto paesi non UE.

Le regole per il trasferimento dei dati da parte dell'Europol a paesi terzi sono indicate nel regolamento di Europol. Secondo queste regole, accordi internazionali negoziati e conclusi dalla Commissione avrebbe fornito la base giuridica necessaria per lo scambio di dati personali tra Europol e le autorità di questi otto paesi, con l'obiettivo di combattere la criminalità grave e il terrorismo.

Il GEPD ha emesso un [Opinione](#) sulle raccomandazioni della Commissione il 14 marzo 2018. Abbiamo sottolineato che gli accordi internazionali in materia di scambio di dati tra l'Europol e paesi non UE devono trovare un giusto equilibrio tra la necessità di combattere la criminalità grave e il terrorismo e la necessità di proteggere i dati personali e altri diritti fondamentali. Ogni accordo deve anche delineare le condizioni specifiche nelle quali Europol può trasferire dati personali al paese interessato, riconoscendo che tali condizioni saranno diverse per ogni paese.

Abbiamo fornito alcune raccomandazioni generali volte a garantire che gli accordi negoziati comprendono le opportune garanzie richieste dal regolamento di Europol, ma abbiamo principalmente concentrati sugli allegati alle raccomandazioni della Commissione. Questi stabiliscono i mandati e le direttive del Consiglio dovrebbe dare alla Commissione per negoziare ogni accordo. In quanto includono tutte le esigenze di protezione dei dati con i quali gli accordi internazionali dovrebbero conformarsi, abbiamo fornito raccomandazioni su come garantire che tali requisiti fossero ampia portata.

### Semplificare la cooperazione giudiziaria in materia di famiglia

Il regolamento Bruxelles II bis è un regolamento del Consiglio relativo agli ioni di jur isdict. Riguarda l'ione recognit e l'esecuzione delle decisioni in materia matrimoniale e ters mat di genitori ty responsa Li,

Compreso sottrazione internazionale di minori. Il Consiglio ha chiesto formalmente un GEPD [Opinione](#) su una proposta di rifusione del regolamento, che abbiamo pubblicato il 15 febbraio 2018. Abbiamo poi presentato questo al Consiglio il 1 Marzo 2018.

La rifusione del regolamento Bruxelles II bis stabilisce la giurisdizione uniforme su regole per il divorzio, la separazione e l'annullamento del matrimonio, così come per le controversie sulla responsabilità genitoriale in situazioni transfrontaliere. Il suo obiettivo principale è quello di rimuovere i **rimanenti ostacoli alla *movimento Libero* delle decisioni giudiziarie, in linea** con il principio del riconoscimento reciproco, e per proteggere meglio gli interessi dei bambini semplificando le procedure e migliorando l'efficienza. Le nuove norme mirano anche al fine di evitare la creazione di una nuova banca dati UE IT, migliorando la cooperazione tra le autorità centrali coinvolte nello scambio di informazioni all'interno e tra gli Stati membri.

A nostro parere abbiamo fornito raccomandazioni specifiche per garantire che qualsiasi trattamento dei dati personali viene effettuato in modo lecito e che le misure di salvaguardia adeguate e specifiche sono messi in atto per tutelare i diritti fondamentali e gli interessi delle persone interessate. Abbiamo anche raccomandato che le clausole di spiegare gli scopi specifici per i quali i dati possono essere trattati, e gli individui questo riguarda, essere inserita nel testo, oltre ai riferimenti espliciti alla necessità di rispettare i principi della qualità dei dati e la riduzione al minimo.

Per garantire che i dati vengono elaborati in modo coerente ed equo in tutta l'UE, abbiamo ribadito la necessità di specificare che ogni riferimento alla legislazione nazionale di uno Stato membro non dovrebbe portare ad un aumento dei limiti alla destra di un individuo di informazioni a livello nazionale. Abbiamo anche consigliato che stabilisce un principio nel regolamento per fornire agli individui con il diritto di accedere a qualsiasi informazione trasmessa all'autorità richiedente di uno Stato membro. Per far fronte a situazioni in cui risultano necessarie restrizioni all'accesso e di rettifica dei diritti di un individuo, abbiamo espresso la necessità di una disposizione specifica che delinea la portata di queste restrizioni.

## 4.4. PER TERRA

Il GEPD ha il compito di garantire che le istituzioni dell'UE sono conformi alle norme di protezione dei dati sia quando trattano dati personali se stessi e quando si sviluppano nuove politiche dell'UE. Nel caso del primo, significa che funge da autorità di controllo per tutte le istituzioni e gli organi dell'UE, mentre il secondo vede il GEPD adottano il ruolo di consulente per il legislatore dell'UE.

Gran parte del nostro lavoro nel 2018 mira a garantire che sia il GEPD e l'UE istituzioni e degli organismi che supervisionano sono stati preparati per la [nuove regole sulla protezione dei dati](#), Che è diventato pienamente applicabile l'11 dicembre

2018. In linea con i punti d'azione di cui la [strategia GEPD](#), Una particolare attenzione del nostro lavoro è stato in

crescente **responsabilità**, Assicurando che tutte le istituzioni dell'UE, compreso il GEPD, sono in grado non solo di rispettare le norme sulla protezione dei dati, ma di dimostrare tale conformità.

Oltre a questo, abbiamo continuato ad adempiere ai nostri obblighi standard, come autorità di vigilanza per le istituzioni dell'UE. Questi includono il rilascio di raccomandazioni ai singoli istituti, sotto forma di **controllo preventivo Economia**, Si occupano di **denunce, contestazioni**, La realizzazione di visite regolari audit e di compliance e di fornire corsi di formazione relativi al nuovo regolamento.

Un secondo punto d'azione stabilito nella strategia impegna il GEPD ad agevolare politiche responsabile e consapevole. Tra gli strumenti che **abbiamo per fare questo sono i nostri opinioni e formali Commenti**. Questi ci consentono di fornire raccomandazioni specifiche sulle proposte legislative dell'UE. I nostri sforzi nel 2018 inclusi 11 Opinioni, 14 insiemi di osservazioni formali e oltre 30 consultazioni informali su progetti di proposte da parte della Commissione. Questi numeri dimostrano chiaramente la crescente necessità di, e la pertinenza della, consulenza di esperti indipendenti sulle implicazioni per la protezione dei dati di iniziative dell'UE, nonché un crescente interesse da parte degli stakeholder istituzionali dell'UE.

Con le nuove tecnologie che appaiono ogni giorno, siamo impegnati a garantire che il campo di protezione dei dati prende le misure **necessarie per adattare all'era digitale. iniziative GEPD come il Internet Privacy rete Ingegneria (IPEN) mirano a rafforzare le nuove regole stabilite nel Il regolamento generale sulla protezione dei dati**

(GDPR) e incoraggiare lo sviluppo di tecnologie che rispettino Privacy-.

Ci rendiamo conto che la protezione dei dati da sola non può risolvere tutti i problemi, in modo da garantire che la protezione dei dati va digitale abbiamo anche concentrati sullo sviluppo di soluzioni politiche interdisciplinari. Attraverso iniziative come la stanza di compensazione digitale, per esempio, speriamo di incoraggiare una maggiore cooperazione tra le autorità di protezione dei dati e la protezione dei consumatori al fine di garantire i diritti delle persone siano adeguatamente protetti.



#### 4.4.1 La funzione DPO: istituzioni dell'UE guidare con l'esempio

**Responsabili della protezione dei dati (DPO)** dalle 66 istituzioni, gli organi, le agenzie e gli uffici si incontrano con il GEPD due volte l'anno, come parte dei loro incontri di rete RPD. Questi incontri rafforzano la collaborazione tra gli RPD e garantire che le istituzioni dell'UE hanno gli strumenti necessari per dare l'esempio nell'applicazione della legge sulla protezione dei dati.

Con le nuove norme di protezione dei dati per le istituzioni dell'UE in discussione, incontri recenti si sono concentrati quasi esclusivamente su come aiutare gli RPD per garantire che essi siano pronti per le nuove regole. primo incontro di quest'anno, che ha avuto luogo a Bruxelles il 31 maggio 2018, non ha fatto eccezione.

**Solo una settimana prima del 43<sup>o</sup> incontro DPO, il GDPR diventato** pienamente applicabile e il Consiglio ha annunciato un accordo politico con il Parlamento europeo su una GDPR per le istituzioni dell'UE (**vedere la sezione 4.1.2**). Non sorprende quindi, le attività della giornata focalizzata sulla necessità di garantire che DPO erano dotati di tutte le conoscenze e gli strumenti necessari non solo per garantire il rispetto delle nuove regole, ma per dimostrare tale conformità, attraverso l'applicazione del principio di responsabilità. Con l'obiettivo di fornire loro con esempi pratici di come applicare le nuove regole, RPD ha partecipato a diversi scambi interattivi, focalizzata su casi di studio specifici. Questi trattati molti argomenti, tra cui i social media e il targeting micro, di impatto sulla protezione dei dati (valutazioni DPIAs) e IT governance.

Per fornire ulteriore sostegno ai RPD nella transizione verso le nuove **regole, il 30 settembre 2018 abbiamo pubblicato un versione aggiornata del** nostro giornale 2.005 posizione sul ruolo degli RPD all'interno delle istituzioni europee. Questo documento riguarda anche il loro rapporto con il GEPD e fornisce le linee guida sul profilo di un DPO e le risorse necessarie per svolgere al meglio il proprio ruolo. La versione aggiornata porta la carta in linea con le nuove norme stabilite nel regolamento 2018/1725 e incorpora un **feedback da DPO, raccolte nel corso di un periodo di consultazione in primavera 2018.**

Le nuove regole si applica integralmente in data 11 dicembre 2018. Il 12 dicembre 2018, DPO riuniti ancora una volta a Bruxelles per il 44 ° incontro GEPD-DPO. L'incontro è stato l'occasione per riflettere sulle nuove sfide affrontate dal GEPD e DPOs dalla nuova normativa.

Abbiamo pianificato le attività della giornata intorno ad una serie di studi di casi finalizzati a fornire le DPOs con esperienza pratica di come affrontare alcune di queste nuove sfide. Tra queste, la restrizione degli individui

diritti in base alle nuove regole, i dati sulle notifiche di violazioni e responsabilità condivisa. Volevamo incoraggiare RPD per vedere le nuove regole non come un peso, ma piuttosto come uno strumento di riferimento su come garantire il rispetto dei diritti degli individui i cui dati personali le istituzioni europee utilizzano quotidianamente per svolgere i propri compiti e responsabilità.

Prima di entrambe le riunioni DPO, abbiamo organizzato una sessione di formazione complementare per DPO recentemente arredate e Assistente DPO. I nuovi RPD sono stati dati informazioni utili circa il loro ruolo e le responsabilità, che termina la giornata con uno studio pratico caso di mettere le loro conoscenze in pratica.



#### 4.4.2 Rafforzare la responsabilità delle istituzioni UE

Sia il GDPR e le nuove regole sulla protezione dei dati per le istituzioni dell'UE sottolineano l'importanza di responsabilità. Questa è l'idea che il titolare del trattamento, la persona o l'organizzazione responsabile del trattamento dei dati personali, deve rispettare non solo le norme sulla protezione dei dati, ma essere in grado di dimostrare tale conformità. Non è un concetto nuovo, ma le nuove regole porre maggiore enfasi su di esso.

Responsabilità tratta di fare la cosa giusta, per le ragioni giuste, in un modo che può essere riprodotta, se necessario. Al fine di rendere questo una realtà, ogni organizzazione che opera all'interno della UE, tra cui le istituzioni dell'UE, deve garantire che essi adeguatamente documentare tutte le loro attività di trattamento dei dati.

Per aiutare le istituzioni dell'UE a questo, abbiamo emesso un [la responsabilità sul toolkit terra](#). Una versione preliminare del kit di strumenti è stato pubblicato nel mese di febbraio 2018, per aiutare le istituzioni dell'UE nei loro preparativi per la

nuove regole. Una versione aggiornata, che riflette con precisione la versione finale del nuovo regolamento 2018/1725, è stato rilasciato nel mese di dicembre 2018, in coincidenza con il giorno in cui le nuove norme si applica integralmente.

Il toolkit fornisce indicazioni su come documentare un'operazione di trattamento, attraverso ciò che è noto come record. Esso stabilisce anche i criteri per determinare se un DPIA, o valutazione di soglia, è necessario.

Il toolkit integra il lavoro sulla responsabilità che abbiamo fatto con gli RPD ([vedere la sezione 4.4.1](#)), Così come i corsi di formazione e visite di responsabilità che abbiamo svolto negli ultimi due anni per preparare le istituzioni per il nuovo regolamento ([vedere la sezione](#)

[4.1.2](#)).

#### 4.4.3 Responsabilità in IT

Due mesi prima della GDPR è diventata esecutiva, abbiamo pubblicato due nuovi set di linee guida. Queste linee guida forniscono le istituzioni dell'Unione europea con consigli su come adattarsi a questa nuova era nella protezione dei dati, notevole per l'accento posto sul principio di responsabilità.

I requisiti di protezione Linee Guida per l'indirizzo dei dati [la gestione e la governance delle infrastrutture IT](#) in generale, e per [servizi di cloud computing](#) nello specifico. Pubblicato prima che le nuove regole per le istituzioni dell'UE erano stati ultimati, gli orientamenti si basano sui principi enunciati nella GDPR e completare gli altri sforzi per preparare le [istituzioni dell'UE per le nuove regole](#) ([vedere le sezioni 4.1.2](#), [4.4.1 e 4.4.2](#)).

Sosteniamo pienamente l'idea che le istituzioni dell'UE dovrebbero beneficiare dei più recenti sviluppi tecnologici. In questo modo si assicura che l'amministrazione dell'UE è sia efficiente e trasparente. Le linee guida mirano a dimostrare che questo può essere fatto, pur mantenendo il pieno rispetto dei diritti fondamentali. Essi identificano chiaramente i limiti che devono essere rispettati.

Prima della pubblicazione di queste linee guida, siamo stati invitati a un [seminario sulla sicurezza del trattamento dei dati personali](#) per presentare la nostra guida provvisoria per le istituzioni dell'UE in materia di documentazione e obblighi relativi al DPIAs e il ruolo svolto dalla [la gestione dei rischi di sicurezza IT](#) in questo.

Organizzato dall'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) e l'italiano [autorità per la protezione dei dati \(DPA\)](#) Garante, il workshop si è svolto a Roma l'8 febbraio 2018. Un focus della discussione è stata la necessità per le organizzazioni di integrare meglio la gestione dei rischi di protezione dei dati personali nei loro metodi di lavoro.

L'integrazione di nuovi obblighi in materia di entrambi i DPIAs e sicurezza IT in un processo di gestione del rischio comune che si rivolge sia rischi per la sicurezza informatica e la protezione dei dati è senza dubbio una sfida. Tuttavia, evita la duplicazione e consente una più corretta attuazione degli obblighi delineati nel GDPR, rendendo molto più efficiente rispetto all'implementazione processi separati.



#### 4.4.4 dati notifiche di violazione: un how-to guida per le istituzioni dell'UE

Per aiutare le istituzioni dell'UE con i loro preparativi per le nuove regole (vedere le sezioni 4.1.2, 4.4.1 e 4.4.2) Abbiamo emesso **ines Guidel sulla notifica delle violazioni dei dati personali**.

In base al nuovo regolamento, tutte le istituzioni e gli organi dell'UE hanno il dovere di segnalare alcuni tipi di violazioni di dati personali al GEPD. Essi devono farlo entro 72 ore dalla presa di coscienza della violazione. Se v'è un elevato rischio che la violazione negativamente i diritti e le libertà degli individui Fect af, l'istituzione UE deve anche informare le persone interessate senza inutili ritardi.

I costi ed i rischi legati alla violazione dei dati può essere significativo. Dal momento che la prima legge di notifica delle violazioni dei dati obbligatoria è stata approvata in California nel 2002, l'obbligo di comunicazione diversi tipi di violazioni si è diffuso in tutto il mondo, in risposta ad un crescente numero di incidenti. Tale obbligo non solo dovrebbe fungere da deterrente, ma incoraggiare anche le organizzazioni a fare tutto quanto in loro potere per impedire le violazioni che si verificano in luogo f irst. rigorosi requisiti del GDPR sulle notifiche di violazioni di dati hanno già dimostrato gli effetti positivi di questo approccio.

Con il nuovo regolamento sulla protezione dei dati per le istituzioni comunitarie attualmente in vigore, le istituzioni devono assicurare di avere meccanismi di prevenzione e rilevamento in

posto per violazioni dei dati personali, nonché le procedure di indagine e di reporting interno. I nuovi orientamenti prevedono la necessaria consigli pratici e lo sfondo le informazioni per valutare e **notificare il GEPD attraverso un nuovo modulo online**, Che può essere **trovato su il nostro sito web**.

#### 4.4.5 La tutela della privacy nelle istituzioni dell'UE

Uno dei principali compiti del GEPD è quello di ascoltare e indagare sulle denunce e condurre indagini.

Nel 2018, il GEPD ha ricevuto 298 denunce, con un incremento del 111% rispetto al 2017. Di questi, 240 denunce sono state inammissibile, la maggioranza relativa al trattamento dei dati a livello nazionale, a differenza di trattamento da parte di un'istituzione o un organismo comunitario.

I restanti 58 reclami richiesto un'indagine approfondita, un incremento del 132% rispetto al 2017.

Inoltre, 38 casi presentati negli anni precedenti erano ancora nella richiesta, rivedere o di follow-up fase il 31 dicembre 2018 (uno in 2012, sette nel 2014, tre nel 2015, dodici nel 2016 e quindici nel 2017). Nel 2018 abbiamo pubblicato 23 decisioni di denuncia.

#### protezione dei dati per l'organizzazione di conferenze

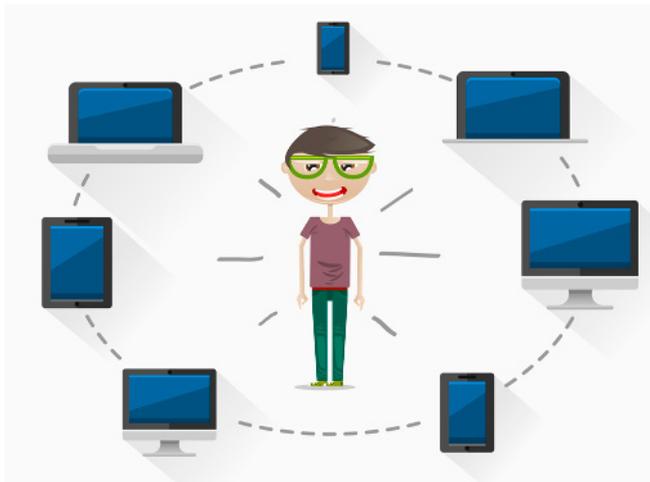
Il 10 aprile 2018, abbiamo risposto ad una denuncia per quanto riguarda il processo di registrazione per una conferenza internazionale organizzata da una delle istituzioni dell'UE. Questo processo richiede alle persone di presentare una copia scannerizzata del passaporto o carta d'identità, al fine di verificare la loro identità.

La nostra indagine ha rilevato che l'istituzione UE avrebbe potuto usare un mezzo meno invasivo di verificare l'identità dei partecipanti, come il controllo passaporti o carte d'identità all'ingresso della conferenza e confrontandoli con le informazioni presentate on-line. Abbiamo anche notato che in alcuni Stati membri è illegale a fotocopiare i passaporti a meno giustificato dalla legge.

Inoltre, l'istituzione europea ha omesso di notificare formalmente la loro DPO della collezione di copie scannerizzate di ID degli individui, come è stato richiesto in **Regolamento**

**45/2001**, Le regole di protezione dei dati applicabili alle istituzioni comunitarie, al momento della denuncia.

Abbiamo anche risposto alle preoccupazioni circa il trasferimento alle autorità dello Stato membro ospitante dei dati personali raccolti dagli organizzatori della conferenza. L'istituzione dell'UE ha affermato che questo trasferimento è stato effettuato sulla premessa che i partecipanti avevano acconsentito ad esso. Tuttavia, per qualificarsi come una base giuridica valida per il trasferimento dei dati, il consenso deve essere dato liberamente. Come partecipanti non sono stati in grado di registrare per questa conferenza, a meno hanno dato il loro consenso a condividere informazioni personali con le autorità dello Stato membro ospitante, il loro consenso non è stato dato liberamente. Di conseguenza, il consenso, in questo caso, non può essere considerato un valido fondamento giuridico per il trasferimento di dati.



#### Il trattamento dei dati per il monitoraggio dei social media

Il 21 marzo 2018, abbiamo adottato un **Opinione** sul trattamento dei dati personali per il monitoraggio dei social media presso la Banca centrale europea (BCE). La BCE intendeva usare un contraente esterno per monitorare e tenere traccia di discussioni su argomenti correlati della BCE su diversi canali di social media. Il loro scopo era quello di ottenere una migliore comprensione di come gli utenti internet percepiscono la BCE e per migliorare la comunicazione e la reputazione della BCE.

In particolare, la BCE ha voluto raccogliere informazioni su ciò che è stato detto su di loro, argomenti legati alla loro attività, il tono usato e in che misura le informazioni

è stato diffuso. Il monitoraggio e l'analisi dei dati aggregati sui diversi gruppi di utenti doveva essere effettuata dal contraente esterno, mentre la BCE analizzava queste informazioni e progetti di relazione.

Come alcuni utenti di Internet, che non sono personaggi pubblici, possono essere indirettamente identificabili per le loro quotazioni, le loro simpatie o la loro lingua madre, abbiamo fornito la BCE con alcune raccomandazioni specifiche volte a garantire che i diritti dei singoli sarebbero stati rispettati. In particolare, ci siamo concentrati sulla necessità di garantire la qualità dei dati con il GDPR e trasformati, provando a DED raccomandazioni sul contenuto del contratto con il contraente esterno e ha consigliato la BCE sulla destra un individuo di accesso al proprio propri dati. Abbiamo inoltre fornito loro con consigli sulle informazioni che devono fornire agli utenti internet e le misure di sicurezza il contraente dovrà adottare.

Il 13 novembre 2018, abbiamo effettuato un sopralluogo in situ presso la BCE e siamo rimasti molto felici di notare che la BCE aveva messo le nostre raccomandazioni in pratica. In additione, quasi tutti i dati utilizzati dalla squadra comunicazione BCE sta aggregati.

Ai sensi del regolamento 45/2001, tutte le operazioni di trattamento che possono presentare rischi specifici per i diritti e le libertà delle persone in virtù della loro natura, oggetto o finalità dovevano sottoporre a controllo preventivo da parte del GEPD.

Nel 2018, abbiamo ricevuto dieci notifiche di controllo preventivo, una riduzione del 92% sul 2017. Abbiamo rilasciato 90 precedenti di controllo Opinioni, con un incremento del 55% rispetto al 2017. Di questi, sette sono stati Controlla opinioni non-precedenti e tre sono stati aggiornati Opinioni seguito aggiornato notifiche. Il 90% delle operazioni di trattamento rischiose che ci sono state notificate circa nel 2018 relative alle procedure amministrative, come ad esempio l'assunzione di personale, valutazioni annuali del personale o la conduzione delle indagini amministrative e i procedimenti disciplinari, come è stata la tendenza negli anni passati.

## Numero di reclami ricevuti

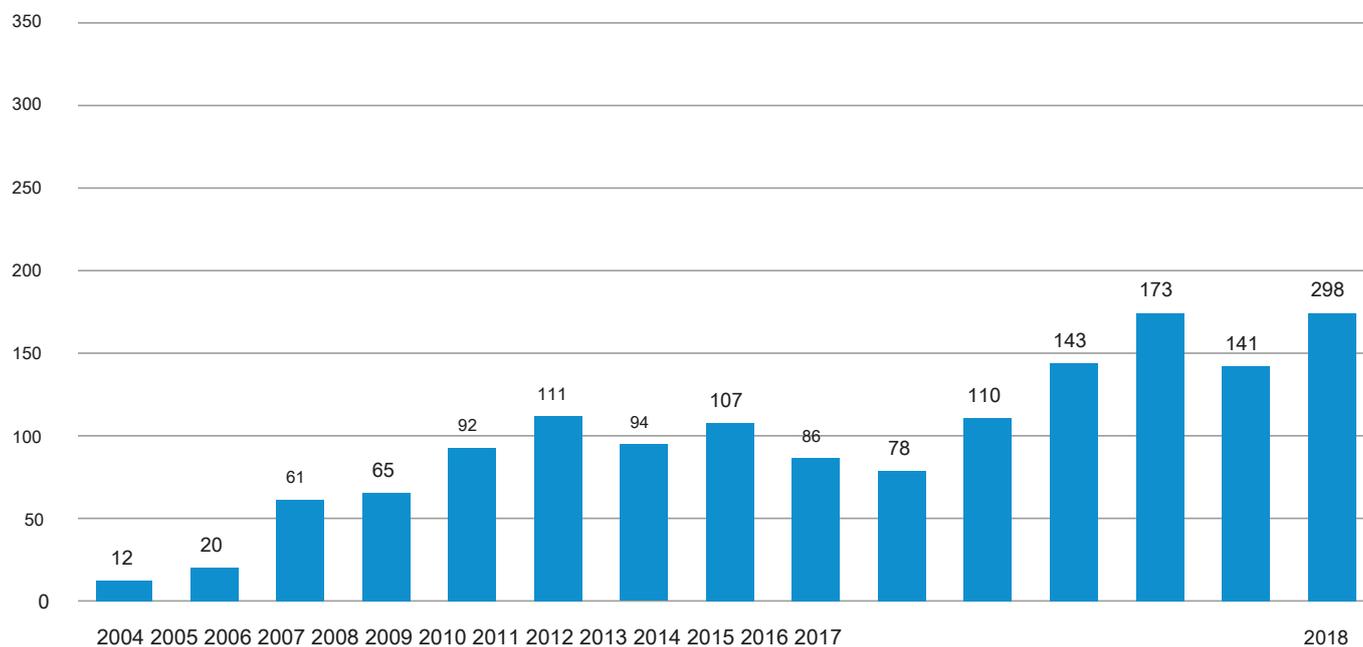


Figura 3. Evoluzione del numero di denunce, tra cui denunce irricevibili, ricevuto dal GEPD

## le istituzioni e gli organi dell'UE interessati

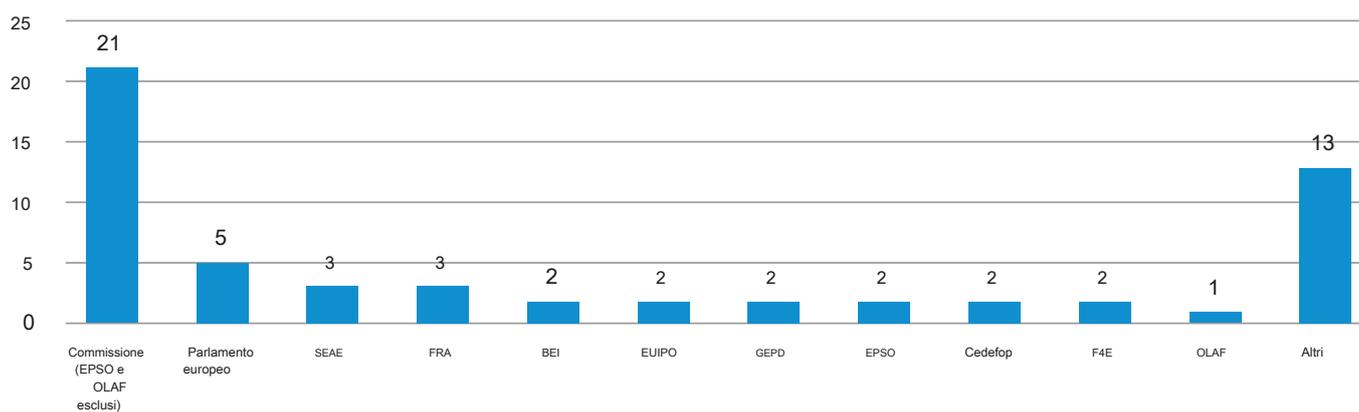


Figura 4. istituzioni e gli organi interessati da denunce ricevute dal GEPD UE

## Argomenti di reclami 2017

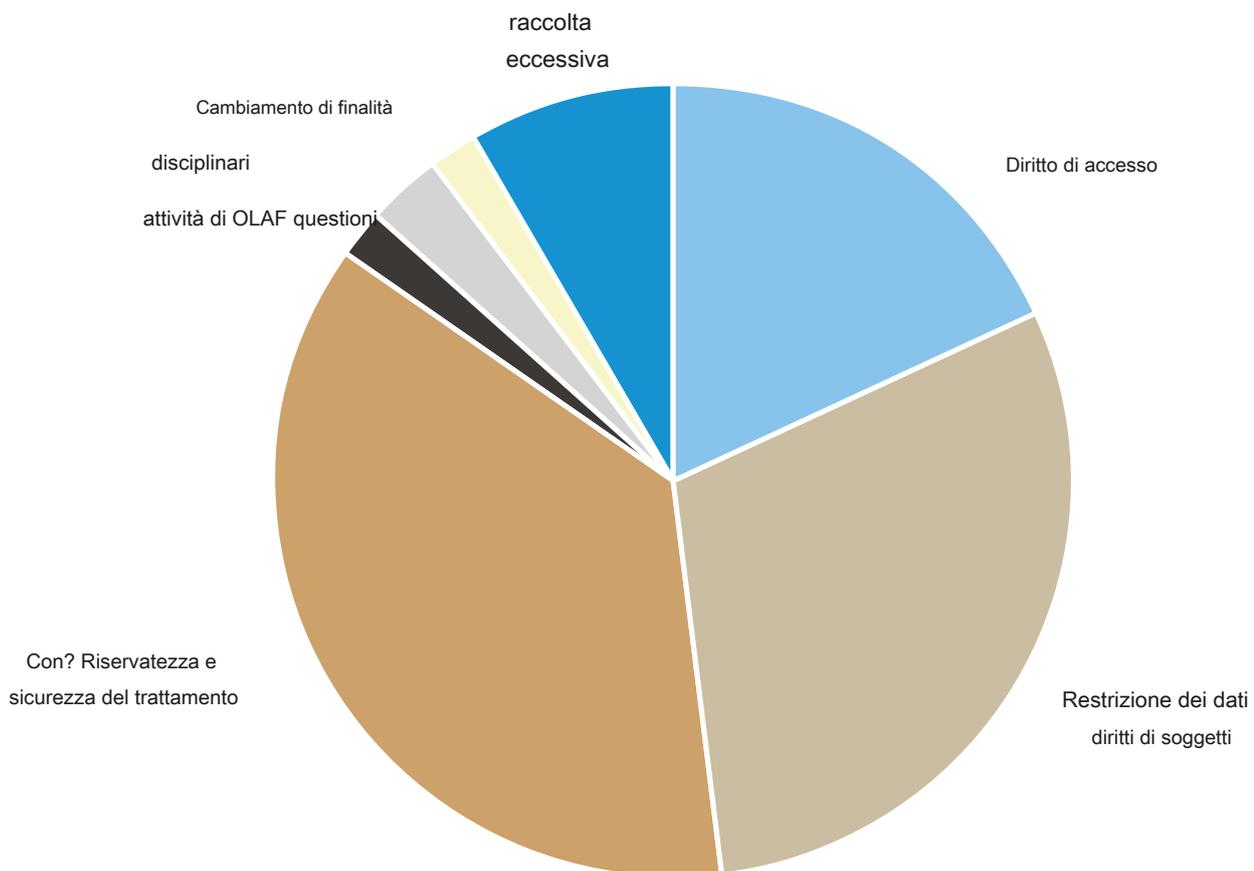


Figura 5. Tipo di violazione presunta dei reclami ricevuti da GEPD

Nel 2018 abbiamo ricevuto dieci consultazioni sulle misure amministrative (otto ai sensi degli articoli 28.1 del regolamento 45/2001 e due ai sensi dell'articolo 41 del regolamento 2018/1725).

Abbiamo ricevuto 30 consultazioni, (29 di cui all'articolo 46 (d) del regolamento 45/2001 e uno ai sensi dell'articolo 57 (1) g del regolamento 2018/1725), otto dei quali erano consultazioni informali.

### controllership comune: il caso dello strumento di supporto linguistico online

Erasmus + è il programma della Commissione europea per l'istruzione, la formazione, la gioventù e lo sport. L'istruzione, gli audiovisivi e la cultura (EACEA) esegue il programma per la direzione generale della Commissione europea per l'Istruzione e la Cultura (DG EAC), al fianco di agenzie nazionali degli Stati membri.

Come parte del programma Erasmus +, EACEA gestisce uno strumento online conosciuto come supporto linguistico online (OLS). È usato per controllare se le competenze linguistiche di un individuo sono migliorate durante il loro soggiorno all'estero. Le competenze linguistiche sono testate sia prima che un individuo lascia il loro paese d'origine e al loro ritorno a casa. OLS fornisce anche corsi di lingua on-line. I test sono obbligatori per ogni individuo che riceve finanziamenti attraverso Erasmus +, ma le conseguenze in materia di non aver preso il test, come ad esempio una riduzione della borsa di mobilità di un individuo, sono decise a livello nazionale.

Qualsiasi trattamento di dati personali proposti da un'istituzione o un organismo UE e considerate rappresentare un rischio specifico per i diritti e le libertà delle persone interessate è soggetta a controllo preventivo da parte del GEPD. Tuttavia, mentre EACEA fornisce lo strumento on-line, che non effettua una valutazione dei dati raccolti dallo strumento. Questo viene fatto a livello nazionale. Abbiamo quindi informato EACEA che nessun controllo preliminare è necessario in questo caso.

## Comunicazioni alla GEPD

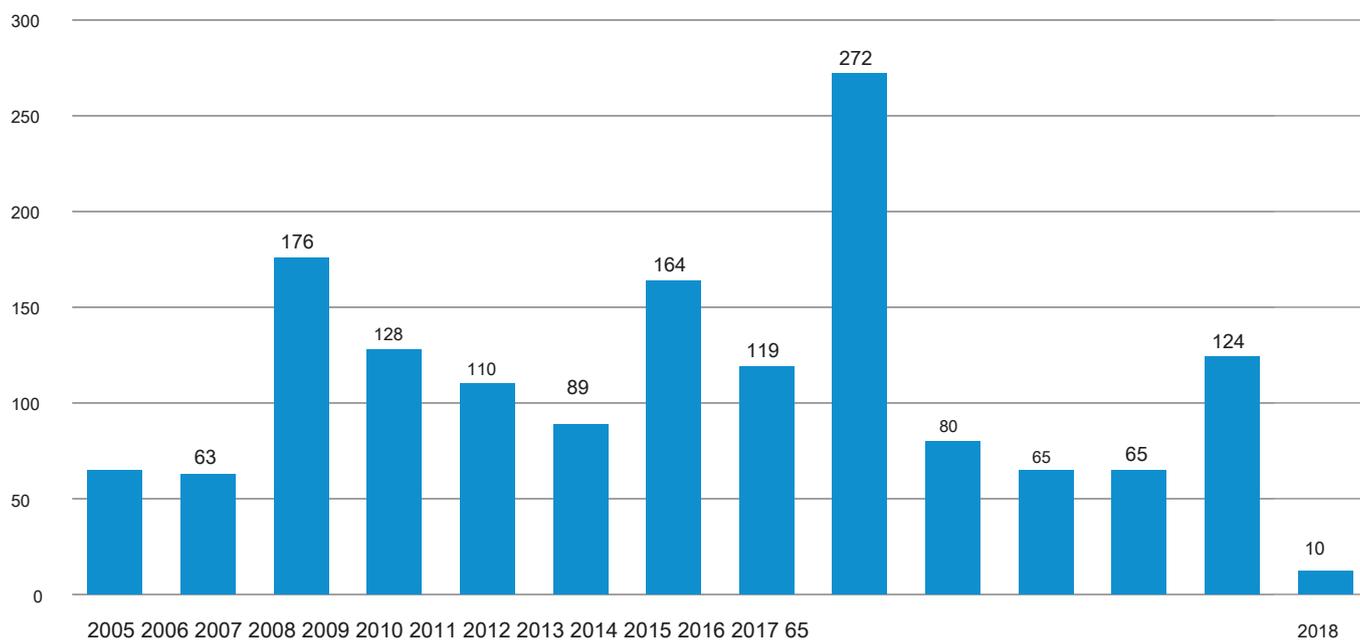


Figura 6. Evoluzione delle notifiche ricevute dalla GEPD

## Opinioni GEPD di controllo preventiva all'anno

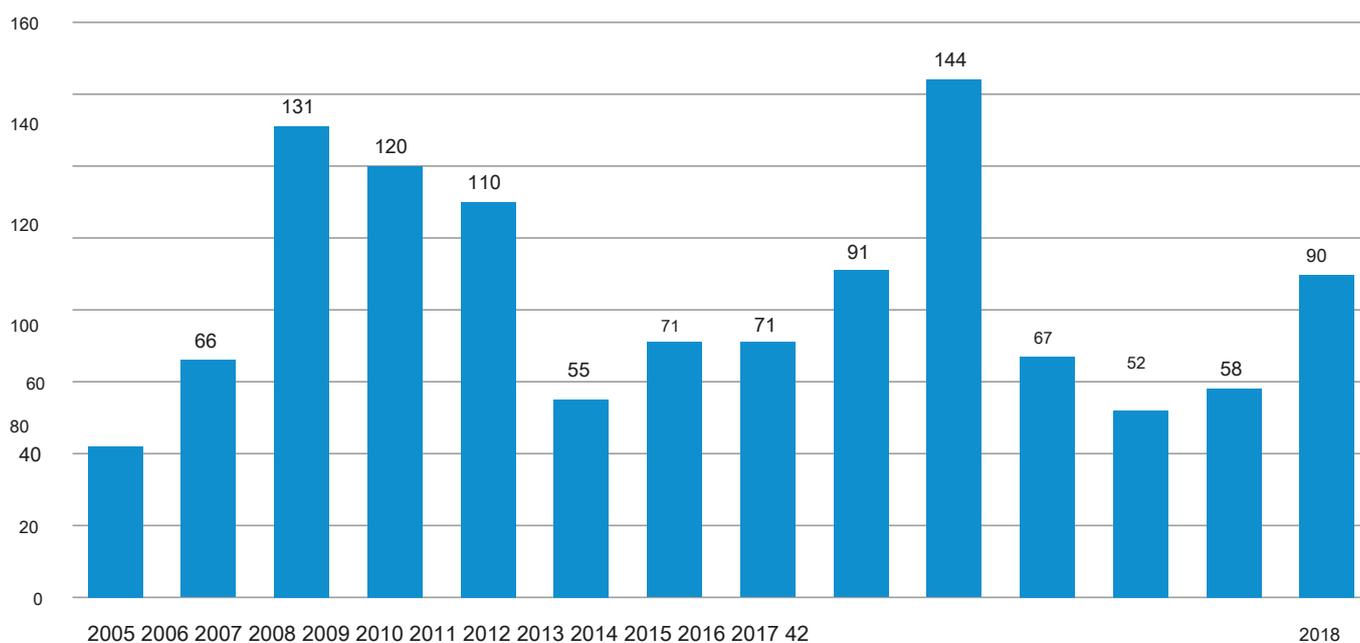


Figura 7. Evoluzione delle opinioni di controllo preventivo rilasciate da GEPD

## Comunicazioni alla GEPD 2018 Core Business Administration vs

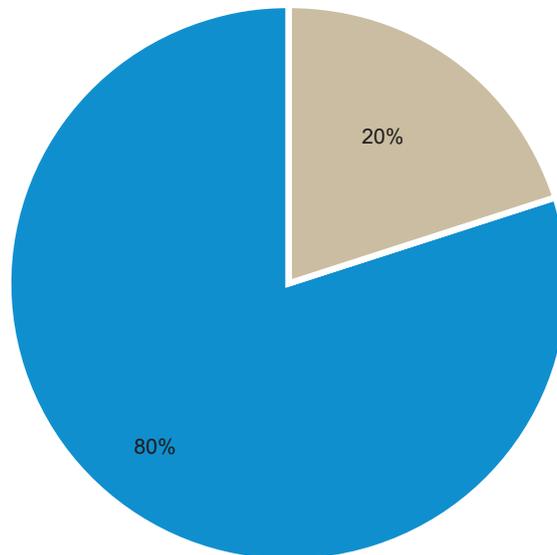


Figura 8. Percentuale scissione tra core business e le attività di amministrazione nelle notifiche ricevute dal GEPD

Il caso ha sollevato una questione interessante, però, che è importante per molti sistemi, piattaforme e strumenti europei.

Il GEPD vede la ripartizione dei compiti tra EACEA e DG EAC, da un lato, e le agenzie nazionali, dall'altro, come un caso di responsabilità condivisa. Ciò significa che sia UE e le autorità nazionali sono responsabili per la determinazione dei mezzi e finalità del trattamento dei dati personali. Si consiglia, pertanto, che questi controller comuni chiarire le rispettive responsabilità, in modo che sia possibile per gli individui per affrontare subito la giusta organizzazione, a seconda delle loro esigenze. Ad esempio, nel caso della OLS, le richieste di accesso ai dati personali relativi ai risultati dei test devono essere indirizzate all'agenzia nazionale del paese di origine di un individuo, mentre la sicurezza del sistema centrale OLS rimane la responsabilità di EACEA.

### UE sindacati e il GEPD

Il 29 gennaio 2018, abbiamo risposto ad una consultazione da un sindacato per il personale dell'UE, relativa alle condizioni per la condivisione dei dati all'interno dello stesso sindacato.

Il nostro parere scoperto che questi sindacati non sono classificati come istituzioni o organi dell'UE sotto la relativa disposizione delle regole per le istituzioni e gli organi dell'Unione europea, di cui al momento ai sensi del regolamento 45/2001.

Tuttavia, come regola generale, qualsiasi trasferimento interno dei dati dovrebbe essere governata dal principio della necessità di sapere. Abbiamo quindi consigliato il sindacato di effettuare un'analisi per determinare se i trasferimenti di dati interni, peraltro necessario in questo caso.

### siti web delle istituzioni UE devono dare l'esempio

Il GEPD ha ricevuto una serie di denunce relative alla tutela della privacy e dei dati personali sui siti web di alcune istituzioni e degli organismi dell'UE. Questi reclami relativi a:

- l'utilizzo di servizi di terze parti;
- il consenso dell'utente in materia di cookie;
- le informazioni fornite agli utenti del sito web nella politica cookie del sito web;
- le informazioni fornite agli utenti nelle norme sulla privacy del sito.

Abbiamo lavorato a stretto contatto con le istituzioni interessate per risolvere eventuali questioni sollevate nelle denunce. Questo si adatta con i nostri sforzi più ampi per aiutare tutte le istituzioni e gli organi dell'UE garantiscono il rispetto delle leggi sulla protezione dei dati, tra cui i nostri tentativi per aiutarli a meglio proteggere gli utenti del

i loro siti web. Inclusi in questo è il nostro programma di ispezioni a distanza ( [vedere la sezione 4.4.7](#) ) E l'organizzazione di sessioni di formazione specifici ( [vedi figura 2](#) ), Tra le altre attività. Questi sforzi continueranno nel 2019, il nostro obiettivo è di assicurare che ogni sito web istituzione dell'UE è conforme ai requisiti di protezione dei dati rilevanti.

#### 4.4.6 Facendo con le istituzioni: verifiche e visite

Le verifiche e le visite sono due dei numerosi strumenti che usiamo per monitorare le istituzioni dell'UE e garantire che esse rispettino le norme di protezione dei dati rilevanti. Le visite sono anche uno strumento utile per aiutare ad aumentare la consapevolezza circa la protezione dei dati nelle istituzioni dell'UE e si sono dimostrati particolarmente utili come parte della nostra campagna di sensibilizzazione e contribuire a preparare le istituzioni dell'UE per le nuove regole sulla protezione dei dati ( [vedere la sezione 4.1.2](#) ).

Abbiamo effettuato sette verifiche e tre visite di conformità nel 2018. Con le nuove regole in mente, questi avevano lo scopo di assicurare che le istituzioni europee hanno gli strumenti giusti e le conoscenze di andare oltre il semplice rispetto,

verso l'approccio basato sulla responsabilità delineata nel nuovo regolamento. E' fondamentale che le istituzioni comunitarie sono in grado di dare l'esempio nella loro applicazione delle norme sulla protezione dei dati al fine di contribuire a garantire il successo di tutta l'UE GDPR.

I risultati delle verifiche sono sempre condivisi direttamente con le istituzioni interessate. Abbiamo poi follow-up a tempo debito per garantire che le nostre raccomandazioni sono state messe in pratica. visite di conformità, d'altra parte, coinvolgono lavorare con il rispettivo ente UE di elaborare una tabella di marcia per la conformità. Abbiamo poi seguire con l'istituzione per garantire che la tabella di marcia è stato efficacemente attuato.

In base al nuovo regolamento 2018/1725, continueremo a effettuare verifiche e visite. L'enfasi rimane sul incoraggiando ed assicurando un approccio alla protezione dei dati basato su responsabilità, in linea con le nuove regole.

#### 4.4.7 controlli remoti di webservices

Nel mese di novembre 2016, abbiamo pubblicato [Linee guida](#) in materia di protezione dei dati personali trattati attraverso servizi web di istituzioni dell'UE. Nel mese di luglio 2018, abbiamo

## audit GEPD e visite

2 0 1 8



ha iniziato un esercizio di follow-up, costituita da controlli remoti dei servizi web offerti dalle istituzioni dell'UE.

controlli remoti comportano la scansione remota dei servizi web, e possono quindi essere effettuate nei locali del GEPD. Il nostro approccio è globale, tenendo conto di tutti i servizi web offerti dalle istituzioni dell'UE. Per la prima volta nella storia del GEPD, abbiamo anche automatizzato parte della raccolta delle prove e la documentazione.

Poiché il numero di servizi web segnalati dalle istituzioni ammonta a più di 700, abbiamo organizzato le ispezioni in onde. Ogni onda è composto da un insieme di servizi web, con la prima ondata compresi quei servizi che possono avere il massimo impatto sugli individui che li utilizzano.

La prima ondata di ispezione, che comprendeva i servizi web delle maggiori istituzioni dell'UE, nonché due siti web di Europol (vedere la [sezione 4.2.3](#)), È terminata, mentre la seconda ondata è dovuta a finire nei primi mesi del 2019. Ulteriori ondate di ispezione si svolgerà durante tutto l'anno a venire.

I risultati della prima ondata di ispezione sono stati accolti dalle istituzioni dell'Unione europea, innescando azioni che hanno notevolmente migliorato la loro conformità servizio web. Speriamo di vedere una risposta simile ai risultati di onde futuri.

#### 4.4.8 La trasparenza, il riutilizzo e la protezione dei dati

Forum annuale di quest'anno degli editori ufficiali ha avuto luogo l'8 giugno 2018, a Oslo, Norvegia. La nostra partecipazione a questo evento è una buona opportunità per noi di dimostrare come funziona la protezione dei dati, in pratica, quando applicato alle pubblicazioni ufficiali.

Nel nostro contributo, abbiamo riportato sulla nostra esperienza e competenza come consulente per il legislatore comunitario, come supervisore delle istituzioni dell'UE e come supervisore dell'Ufficio delle pubblicazioni dell'Unione europea in particolare. Il nostro obiettivo era quello di fornire una guida pratica su come garantire il rispetto dei principi di protezione dei dati e le regole quando si tratta di pubblicazioni iciale f.

Ci siamo concentrati su tre argomenti principali volti ad aiutare gli editori a navigare il GDPR:

- Il ruolo degli editori in relazione ai dati personali quando pubblicano per conto delle Corti nazionali, i ministeri della giustizia o parlamenti. Specificamente, abbiamo concentrati sulla chiarire le situazioni in cui la

editore agisce come un controllore di dati personali e quando agiscono come processore.

- Il diritto alla cancellazione, noto anche come il diritto all'oblio, comprese le condizioni alle quali si applica e i limiti di questo diritto.
- Le garanzie di protezione dei dati in atto in caso di riutilizzo delle informazioni del settore pubblico, ha permesso ai sensi della direttiva 2003/98.

L'evento è stato anche l'occasione per migliorare il nostro impegno con la Norvegia, un paese dello Spazio economico europeo (SEE), ai quali si applica il GDPR, e con il Giappone, che ha partecipato alla conferenza per dare una presentazione come un editore ufficiale. Il gruppo ha espresso un interesse ad ascoltare gli aggiornamenti in materia di protezione dei dati come parte delle sue riunioni annuali future.

#### 4.4.9 indagini transfrontaliere di natura diversa

Da quando il GDPR è diventata esecutiva il 25 maggio 2018, alcune istituzioni dell'UE hanno sperimentato problemi di raccolta delle informazioni richieste da alcune società. Queste aziende sostengono che il GDPR impedisce loro di fornire alle istituzioni dell'UE con questi dati. Alcune delle istituzioni e degli organismi interessati da questo problema includono:

- Direzione Generale della Commissione Europea per la Concorrenza (DG COMP), che, tra l'altro, in materia di antitrust;
- l'Ufficio europeo per la lotta antifrode (OLAF), che svolge indagini esterne su sospetti di frode;
- la Banca europea per gli investimenti (BEI) e il Fondo europeo per gli investimenti (FEI), che hanno bisogno di controllare i progetti finanziari.

In risposta a questo problema, abbiamo fatto in modo che le istituzioni dell'UE interessati sono stati pienamente informati sulla legge e come è rilevante per il loro lavoro.

La raccolta dei dati necessari per adempiere il compito assegnato loro dalla legge è legale, e non limitata dal GDPR. L'istituzione dell'UE o organizzazione è tenuto a informare l'interessato che hanno intenzione di trattare i propri dati personali, ma ci sono anche delle eccezioni a questa regola, principalmente in cui informare la persona coinvolta metterebbe a repentaglio le indagini, in particolare nelle sue fasi iniziali.

Tuttavia, il GEPD è in grado di risolvere il problema da solo. Questo perché il problema principale qui riguarda gli obblighi delle imprese, che sono i controllori

sotto la GDPR. Come è il lavoro del DPA nazionali per supervisionare l'aderenza con il GDPR nei loro rispettivi paesi, ci siamo rivolti al Consiglio europeo della protezione dei dati (EDPB) ( [vedere la sezione 4.1.1](#) ) Dare un seguito a questa materia. Speriamo di avere una risoluzione al problema nel più breve tempo possibile.

#### 4.4.10 domanda per il ritorno

Frontex domanda per il ritorno (FAR) è una piattaforma che consente lo scambio di informazioni sui rimpatriati tra il confine europeo e della guardia costiera Agency (Frontex) e gli Stati membri. Rimpatriati sono individui provenienti da un paese non UE considerano soggiornanti illegalmente nell'UE e oggetto di una decisione di rimpatrio emessa da uno Stato membro, sia attraverso una procedura amministrativa o giudiziaria. La piattaforma permetterebbe agli Stati membri di informare Frontex sulle loro operazioni di rimpatrio, compreso il numero di rimpatriati e dove saranno restituiti, così come qualsiasi tipo di assistenza materiale che potrebbero richiedere da Frontex.

Su 26 settembre 2018 abbiamo emesso un parere di controllo preventivo sulla piattaforma FAR. Abbiamo fatto una serie di raccomandazioni, con particolare riferimento al bando di protezione dei dati associato a questa operazione di trattamento e per la necessità di garantire che tutti i rimpatriati sono garantiti i diritti di accesso e di rettifica dei propri dati personali. Abbiamo anche sottolineato la necessità di effettuare valutazioni dei rischi in relazione alla limitazione dei diritti e nel campo della sicurezza informatica e di anonimizzazione.

operazioni di rimpatrio comportano operazioni di trattamento dati in cui l'interessato è particolarmente vulnerabile. E 'quindi fondamentale per garantire che i principi di protezione dei dati siano rispettati al fine di preservare la dignità di queste persone.

#### 4.4.11 verifiche di sicurezza di appaltatori esterni

istituzioni dell'UE utilizzano spesso contraenti esterni per fornire determinati servizi, come la pulizia, la sicurezza o IT. Tuttavia, è essenziale per garantire che questi appaltatori esterni non presentano rischi per la sicurezza. In Belgio, alcune istituzioni dell'UE fanno con la realizzazione di un processo di screening di sicurezza in collaborazione con le autorità belghe.

Anche se un certo numero di istituzioni UE aveva sviluppato le procedure relative a questo processo di screening, altri sono stati meno ben informati. Il 30 ottobre 2018, in risposta ad una richiesta del Servizio europeo per l'azione esterna (SEAE), abbiamo pubblicato un parere sul tema in cui abbiamo delineato una serie di raccomandazioni volte ad aiutare le istituzioni dell'UE.

Il parere ha sottolineato l'importanza di stabilire una base giuridica adeguata per l'attuazione del processo di screening, come quello messo in atto dalla Commissione europea. Istituzioni dell'Unione europea devono inoltre garantire che gli interessati siano adeguatamente informati su come sia l'istituzione dell'UE in questione e le autorità belghe potranno elaborare i loro dati personali e che sono fatti consapevoli del loro diritto di contestare qualsiasi decisione presa contro di loro.

#### 4.4.12 Supervisione l'Autorità di vigilanza EFTA

Nel mese di ottobre 2017, abbiamo preso il ruolo di garante della protezione dei dati per l'Autorità di vigilanza EFTA (ESA). compito principale dell'ESA è quello di garantire che i paesi dell'Associazione europea di libero scambio (EFTA) di Islanda, Norvegia e Lichtenstein rispettare i loro obblighi ai sensi dell'accordo sullo Spazio economico europeo.

normativa UE sulla protezione dei dati si applica anche al SEE. I paesi dell'EFTA sono pertanto tenuti a istituire autorità di controllo nazionale indipendente per far rispettare la GDPR. Tuttavia, il GDPR non si applica alle istituzioni EFTA. Di conseguenza, anche se le istituzioni dell'EFTA si scambiavano i dati personali con la Commissione europea e gli altri organismi dell'UE su base regolare, non erano soggetti ad alcuna regolamentazione sulla protezione dei dati o di supervisione.

Il regime di vigilanza speciale concordato alla fine del 2017 chiuso questo vuoto giuridico. Esso consiste in:

- La decisione ESA 235/16 / COL, in base alle regole di protezione dei dati per le istituzioni europee di cui al regolamento 45/2001, con lievi modifiche in modo da riflettere il contesto giuridico e operativo specifico in cui opera l'ESA. La presente decisione prevede il ruolo di controllo del GEPD.
- Un memorandum d'intesa (MoU) tra l'ESA e il GEPD, che stabilisce le nostre competenze e i compiti della protezione dei dati dell'ESA.

Tuttavia, con l'introduzione di nuove regole per le istituzioni dell'Unione europea, questo regime di vigilanza speciale è ormai fuori moda.

**Nonostante le nostre raccomandazioni al contrario, il regolamento 2018/1725 non copre le norme sulla protezione dei dati o di supervisione per le istituzioni EFTA.**

Con le istituzioni e gli organi dell'UE ora vincolati dalle nuove regole, ne consegue che il regime di protezione dei dati dell'ESA deve essere aggiornato, per portarlo in linea con queste regole. Solo attraverso questo modo saremo in grado di garantire un'adeguata protezione dei dati personali negli scambi con le istituzioni EFTA.

#### 4.4.13 Eurojust: un nuovo ruolo di vigilanza per il GEPD

L'Agenzia dell'Unione europea per la cooperazione giustizia penale (Eurojust) è stato istituito per rafforzare la lotta contro la criminalità organizzata all'interno dell'Unione europea e per promuovere il coordinamento e la cooperazione tra le autorità inquirenti nazionali che si occupano di questi crimini.

Il 6 novembre 2018, il Parlamento europeo e il Consiglio hanno adottato un nuovo quadro giuridico per l'Eurojust. Esso include nuove norme sulla protezione dei dati, che il compito dei GEPD di vigilare sul trattamento dei dati personali presso Eurojust. Esso prevede inoltre la collaborazione tra il GEPD e le DPA nazionali nel quadro del EDPB su qualsiasi questione che richiede partecipazione nazionale, al fine di garantire il controllo coordinato. Le nostre nuove responsabilità di vigilanza avranno inizio il 12 Dicembre, 2019.

Per prepararsi a questo nuovo ruolo di vigilanza, ci coordineremo internamente e organizzare riunioni periodiche con il DPO di Eurojust. I relativi membri del personale del GEPD sarà anche seguire corsi di formazione interni ed esterni relativi alla vigilanza Eurojust.

Una prima visita alla sede di Eurojust all'Aja ha avuto luogo il 29 novembre 2018 e più visite sono previste nel 2019, al fine di assicurare una transizione graduale alla vigilanza GEPD delle attività di trattamento dei dati di Eurojust.

#### 4.4.14 Consulenza alle istituzioni dell'UE



##### elezioni europee libere ed eque

Il 17 dicembre 2018, abbiamo pubblicato un [Opinione](#) sul pacchetto legislativo della Commissione europea sulle elezioni europee libere ed eque. Il pacchetto composto da quattro parti:

- una proposta di regolamento concernente una procedura di verifica per le violazioni delle norme in materia di protezione dei dati personali nel contesto delle elezioni del Parlamento europeo;
- una comunicazione della Commissione europea sulla necessità di garantire elezioni europee libere ed eque;
- una raccomandazione della Commissione europea sulle reti di cooperazione elettorali, la trasparenza on-line e la protezione contro gli incidenti di sicurezza informatica e la lotta campagne di disinformazione relative alle elezioni del Parlamento europeo;
- un documento di orientamento della Commissione europea sull'applicazione della legge sulla protezione dei dati dell'Unione nel contesto elettorale.

A nostro parere, abbiamo riconosciuto il fatto che il pacchetto ha sottolineato il ruolo delle piattaforme di social media nel processo elettorale, nonché la consistenza del pacchetto con la Commissione del [Codice di condotta sulla disinformazione in linea](#).

Con le elezioni del Parlamento europeo fissato per maggio 2019 e numerosi altri elezioni nazionali previste per tutto l'anno, abbiamo riconosciuto la necessità di creare reti elettorali nazionali e una rete di coordinamento europeo, come indicato nella raccomandazione della Commissione. Dato il nostro lavoro in questo settore, abbiamo anche espresso il nostro interesse a partecipare alla rete europea.

Il nostro parere rafforzato l'urgenza della richiesta della Commissione per gli Stati membri per valutare i rischi connessi con le elezioni del Parlamento europeo, in particolare i potenziali incidenti informatici che potrebbero influenzare l'integrità del processo elettorale.

Inoltre, abbiamo ritenuto che, per maggiore chiarezza, un punto di riferimento avrebbe potuto essere incluso al fatto che i dati personali trattati dal Parlamento europeo, l'Autorità per i partiti politici europei e fondazioni politiche europee e del Comitato delle personalità indipendenti sarà effettuata nell'ambito di applicazione del nuovo regolamento per le istituzioni e gli organi dell'UE ([vedere la sezione 4.1.2](#)).

Abbiamo inoltre fornito diverse raccomandazioni specifiche sul regolamento proposto, compresa la necessità di chiarire la portata delle nuove misure e dei loro compiti e la necessità di garantire la riservatezza nello scambio di informazioni tra DPA e del Comitato delle persone indipendenti. Inoltre, abbiamo consigliato compresi i riferimenti alle decisioni del GEPD e l'attuale quadro giuridico di protezione dei dati.



#### Un nuovo patto per i consumatori

Il 5 ottobre 2018, abbiamo pubblicato un [Opinione](#) sul pacchetto legislativo *Un New Deal per i consumatori*. Il pacchetto consisteva nella proposta di direttiva per quanto riguarda una migliore applicazione e la modernizzazione delle norme UE in materia di tutela dei consumatori e la proposta di direttiva sulle azioni rappresentative per la tutela degli interessi collettivi dei consumatori.

Il GEPD ha [costantemente chiamato](#) per un approccio coerente per l'applicazione da parte delle autorità competenti per l'economia digitale e la società. Questi includono dei consumatori, protezione dei dati e autorità garanti della concorrenza. Abbiamo ribadito questo a nostro parere, sottolineando che il diritto dei consumatori e protezione dei dati non può più permettersi di lavorare in insolazione. È necessario un approccio big-picture per affrontare i danni sistemici agli individui nei mercati digitali, coinvolgendo più stretta cooperazione tra esecutori, al fine di evitare l'incertezza giuridica.

Abbiamo accolto con favore l'iniziativa di aggiornare l'applicazione delle norme di consumo e sostenuto l'obiettivo del pacchetto per estendere i benefici per i consumatori che ricevono servizi senza pagare un prezzo monetario. Tuttavia, **con gratuito il prezzo preferito per molti mercati digitali, il consumatore deve** essere protetto indipendentemente dal fatto che un contratto per fornire contenuti o servizi digitali richiede un pagamento o meno.

Sia la legge di tutela dei consumatori e dei dati deve essere cace ef nell'affrontare eventuali danni derivanti dalla digitalizzazione della vita delle persone. I dati personali non possono essere trattati come un bene economico. E 'quindi di vitale importanza per garantire che i dati personali non è menzionato nelle definizioni di contratto per la fornitura di contenuto digitale o di un servizio digitale, in linea con le garanzie previste

dalla [Carta dei diritti fondamentali](#) e il GDPR.

Maggiore allineamento tra consumatori e dei dati richiede politici, così come regolatori, per approfondire il dialogo e comprensione. Iniziative come la stanza di compensazione digitale ( [vedere la sezione 4.4.18](#) ) E le riunioni congiunte del EDPB e la Rete cooperazione per la tutela dei consumatori sono passi fondamentali verso il raggiungimento di questo.



#### Norme in materia di riutilizzo delle informazioni del settore pubblico

Su 10 Luglio 2018 abbiamo pubblicato un [Opinione](#) sulla proposta della Commissione europea di una nuova direttiva sul riutilizzo dell'informazione del settore pubblico (PSI). Nel proporre di modificare il [attuale direttiva](#) , La Commissione stava cercando di agevolare il riutilizzo dell'informazione del settore pubblico in tutta l'UE, armonizzando le condizioni di base per il riutilizzo.

dati PSI include legale, il traffico, meteorologici, economici e finanziari. Il nostro parere fornito raccomandazioni specifiche sul modo di chiarire il rapporto tra la direttiva PSI proposta e le eccezioni indicate nel GDPR. Abbiamo anche affrontato come affrontare il costo di anonimizzazione dei dati e l'uso di DPIAs per *settori sensibili*, come ad esempio l'assistenza sanitaria.

In particolare, abbiamo specificato che precisa formulazione essere utilizzato per chiarire meglio la coerenza tra la direttiva PSI e il GDPR. Inoltre, a causa dei costi elevati associati alla anonimizzazione dei dati personali, abbiamo suggerito che ogni organizzazione che rientrano nel campo di applicazione della direttiva PSI dovrebbe essere in grado di pagare per le spese di anonimizzazione.

Abbiamo anche sottolineato l'importanza di tutelare i diritti delle persone. Mentre può essere vero che più dati che mai sta generati ed elaborati da macchine, gran parte di essa ricade nella definizione di dati personali. Per questo motivo, in particolare evidenziato vari

sfide derivanti dal tentativo di distinguere tra dati personali e non personali.

#### strumenti e processi in materia di diritto societario digitali

Il 25 aprile 2018, la Commissione europea ha adottato una proposta che modifica la direttiva UE 2017/1132 sull'impiego di strumenti e processi digitali nel diritto societario. In risposta alle richieste separate sia dalla Commissione e dal Parlamento, abbiamo pubblicato un

[Opinione](#) sulla proposta il 26 luglio 2018.

La proposta stabilisce regole per la registrazione delle società on-line e l'archiviazione elettronica e la pubblicazione delle informazioni registrate sulle società e rami e quindi comporta lo scambio di dati personali. Ad esempio, le informazioni sul fondatore di una società o il suo direttore potrebbe essere presentata in una registrazione on-line e archiviato elettronicamente.

La proposta prevede inoltre accesso gratuito in tutti gli Stati membri a un elenco di documenti e informazioni, la creazione di un punto di accesso facoltativa alla piattaforma per le istituzioni dell'UE, e introdurrebbe la *una volta sola linea di principio* nel settore del diritto societario. La volta unico principio significherebbe che le aziende avrebbero solo per presentare informazioni pertinenti una volta, da condividere con le diverse autorità, se necessario. I dati personali sarebbero quindi anche essere accessibili alle varie autorità nazionali nei registri delle imprese, nonché in documenti necessari per le operazioni transfrontaliere, quali fusioni, scissioni e conversioni.

Inoltre, la proposta consentirebbe lo scambio di dati sulla squalifica di registri tra i registri delle imprese nazionali. Tale scambio è probabile di coinvolgere i dati relativi alle condanne penali e reati. Poiché questo è considerato come dati sensibili, richiede adeguate garanzie.

Abbiamo delineato diverse raccomandazioni finalizzate ad assicurare il massimo livello di protezione per tutti i dati personali in questione. La proposta è attualmente in fase di negoziazione in seno al Consiglio e al Parlamento europeo.

#### 4.4.15 Nuove tecnologie

##### Blockchain: valutare le implicazioni per la protezione dei dati

*Blockchain* è diventata una potente parola d'ordine nel mondo della tecnologia e innovazione finanziaria. La tecnologia è attualmente utilizzata come catalizzatori di Bitcoin e altri cosiddetti *cripto-valute*, e scatenato lo sviluppo di [Distribuito Ledger Technology \(DLT\)](#).

libri distribuiti quali blockchains sono database con molte repliche sotto il controllo condiviso dei partecipanti distinti, spesso autonoma,.

Originariamente sviluppato per proteggere le transazioni on-line attraverso l'uso di sofisticati crittografia, le industrie ed i legislatori europei stanno ora valutando la possibilità di utilizzare blockchain in una varietà di settori, dalla finanza all'e-government e, anche nel settore sanitario personale. Tuttavia, è fondamentale garantire che tali valutazioni considerano le implicazioni per la protezione dei dati di utilizzo di database distribuiti.

Ogni volta che la tecnologia blockchain viene utilizzato per elaborare i dati personali si applica la legge sulla protezione dei dati rilevanti. Nell'UE, questa legge è il GDPR. Abbiamo seguito l'evoluzione della blockchain dal 2016 e finora ha individuato una serie di sfide alla protezione dei dati, relativi a settori quali la limitazione di stoccaggio, controllership e individuale dei diritti, che cercheremo di approfondire nel 2019.



#### 4.4.16 Privacy ingegneria guadagnando terreno

Nel mese di febbraio 2018, garante Wojciech Wiewiórowski frequentato il Mobile World Congress di Barcellona, uno degli eventi tecnologici più importanti del mondo. Ha partecipato a pannelli e tavole rotonde insieme ad altri commissari di protezione dei dati da tutto il mondo.

L'evento è stata l'occasione per i regolatori di privacy per spiegare come i principi di protezione dei dati possono essere applicati alle nuove tecnologie e di come questi principi la tutela dei diritti fondamentali dei cittadini, ma anche di delineare le loro aspettative in relazione alle misure adottate dal settore a incorporare questi principi in i loro prodotti. I rappresentanti del settore, tuttavia, hanno espresso le loro preoccupazioni che alcuni iniziative legislative potrebbero portare alla restrizione non necessaria dei dati transfrontaliera flussi considerate necessarie per alcune attività commerciali.

Il GEPD ha partecipato a un dibattito con i rappresentanti dell'industria e dei consumatori in materia di trasparenza e di controllo per gli individui nella raccolta e trattamento dei loro dati in Internet delle cose (IOT) ambienti. Abbiamo evidenziato le regole chiare su questo argomento, delineato nel GDPR, e stressed la necessità per i produttori e dispositivi degli oggetti e fornitori di servizi di adottare i principi di protezione dei dati in base alla progettazione e per impostazione predefinita. Per aiutarli con questo, abbiamo invitato a partecipare alla [laboratorio IPEN](#), che ha avuto luogo a Barcellona il 15 giugno 2018, organizzato con il supporto dell'Università Politecnica della Catalogna (UPC).

IPEN è stato istituito dal GEPD nel 2014 per promuovere l'ingegneria privacy e colmare il divario tra legale e IT di ingegneria approcci alla protezione dei dati. Come nel 2017, il workshop 2018 ha avuto luogo subito dopo l'ENISA Annual Privacy Forum. L'obiettivo principale del workshop è stato quello di valutare lo stato di avanzamento delle tecnologie privacy di miglioramento per (PET) sulla scia del GDPR tecnico ing privacy e, e di follow-up sul risultato del laboratorio transatlantica l'anno scorso, che focalizzata sulle esigenze di ricerca e sviluppo nel campo dell'ingegneria privacy.

partecipanti IPEN fornito aggiornamenti sulle iniziative in corso, come il [IPEN wiki](#) su iniziative di standardizzazione relative alla privacy e il deposito di maturità PET. Il rapporto tra etica e sviluppi tecnologici è stato anche un argomento di discussione. Abbiamo sfidato i presenti a pensare di muoversi da privacy by design al concetto di diritti umani da parte di progettazione.

Il Workshop ha fornito l'occasione per le imprese di presentare e dimostrare le soluzioni che combinano innovazione e protezione dei dati. Le aziende come SAP, Qwant e coraggioso condiviso le migliori pratiche su come dare agli utenti un maggiore controllo sui loro dati. Gli accademici ha riferito sui risultati della ricerca recenti e presentato strumenti pratici per aiutare a rilevare problemi di conformità alla privacy e regolatori di supporto e controller per l'attuazione di responsabilità.

Il workshop ha segnato un inizio incoraggiante per l'epoca GDPR. Ci auguriamo di poter continuare questo dialogo interdisciplinare prezioso nel corso dei mesi e anni a venire.

#### 4.4.17 manipolazione online e dei dati personali

Il 20 marzo 2018, abbiamo pubblicato un [Opinione](#) sulla manipolazione on-line e dei dati personali. Il parere ha risposto al dibattito pubblico sulla febbrile *disinformazione*,

responsabile per distorcere la fiducia nel processo democratico. Essa ha sostenuto che il problema fondamentale non è stato il cosiddetto *notizie false*, ma piuttosto l'abuso, su larga scala, dei dati personali e il diritto alla libertà di espressione. Questo abuso è endemica alla

*Informazioni ecosistema digitale* che si è evoluta nel corso degli ultimi due decenni, che è pericolosamente complesso, concentrato e prive di explainability e responsabilità.

Questo ecosistema, spesso definito come l'ecosistema AdTech, dipende da un ciclo di costante monitoraggio, profilazione e il targeting degli individui. Esso ruota intorno a una manciata di potenza straordinariamente ful intermediari plat la forma che, per determinare quali informazioni vengono raccolte sulle persone e presentato di nuovo loro, agire come guardiani efficaci per l'esperienza online della maggior parte delle persone oggi.

Unicamente ad attività commerciali, l'impatto di questo fenomeno sui diritti fondamentali era già significativo. Eppure, come le rivelazioni degli ultimi 12-18 mesi mostrano, questo ecosistema volatilità è stata ora weaponised da attori con motivazioni politiche, tra cui coloro che desiderano interrompere il processo democratico e minare la coesione sociale. Opaco algoritmico contenuti ricompense decisionale che provoca indignazione, sulla base del fatto che una maggiore *Fidanzamento*

genera ricavi per le piattaforme in questione. Questo pone rischi evidenti per i valori fondamentali e della democrazia.

A nostro parere, abbiamo sostenuto che tanto maggiore attenzione è necessaria per il ruolo dei regolatori a lavorare insieme per tenere i giocatori commerciali e politici per tenere conto di come essi elaborano le informazioni personali. Abbiamo identificato un ruolo qui non solo per le DPA, ma anche per le autorità garanti della concorrenza e le autorità di regolamentazione di servizio audiovisive e osservatori elettorali. Nuove regole-privacy sono anche essenziali, per affrontare incentivi di mercato e di aprire lo spazio per i modelli di business alternativi che non dipendono dalla costante sorveglianza e il **targeting invadente** ([vedere la sezione 4.1.3](#)).

Soprattutto, v'è la necessità per il DPA di collaborare meglio con gli altri regolatori, in particolare elettorali e regolatori audiovisivi. Con i timori che le campagne politiche possono essere sfruttando spazi digitali centralizzati e dati ampiamente disponibili per aggirare le leggi esistenti, è di vitale importanza che agiamo per proteggere i diritti e gli interessi degli individui nella nostra società digitale. Si propone pertanto di tenere un workshop nei primi mesi del 2019 e di invitare le autorità di regolamentazione visivi elettorali e audio a partecipare ai lavori Digital Clearinghouse ([vedere la sezione 4.4.18](#)).



#### 4.4.18 Un approccio più coerente alla sfide nel ecosistema digitale: la stanza di compensazione digitale

Ci sono sinergie naturali tra la protezione dei dati, la protezione dei consumatori e la politica di concorrenza. Tuttavia, le autorità incaricate di far rispettare le leggi in questi campi hanno a lungo agito in modo isolato, come se non esistessero queste sinergie. Una maggiore cooperazione tra queste autorità contribuirebbe a migliorare la comprensione delle dinamiche di mercato e di sviluppare risposte più coerenti e consistenti alle sfide poste dall'economia digitale.

La strategia GEPD fa riferimento alla necessità di lavorare oltre i confini disciplinari per affrontare le questioni di politica con una dimensione protezione della privacy e dei dati. In risposta alla nostra propria analisi e le chiamate dai regolatori per stabilire uno spazio di dialogo, abbiamo lanciato il Clearinghouse digitale. I P rima due riunioni del Clearinghouse ha avuto luogo nel 2017.

Il nostro terzo incontro, che ha avuto luogo il 21 giugno 2018, è stata la prima ad accogliere la partecipazione delle autorità al di fuori dell'UE. Regolatori e le agenzie di applicazione di trattati argomenti di interesse a tutte le autorità presenti, tra cui:

- la rilevanza dei dati personali in concorso e l'applicazione dei consumatori;
- l'equità delle politiche sulla privacy e termini e condizioni di servizi gratuiti on-line;
- prezzi di natura collusiva e personalizzato e le teorie connesse di male in mercati digitali;
- la raccolta dei dati non etico e l'analisi a fini di marketing mirato.

Il 10 dicembre 2018, 31 le autorità dell'UE e di altri paesi si sono incontrati per la quarta volta. Abbiamo ampliato il

campo di applicazione della riunione per includere i regolatori elettorali e discusso l'impatto della manipolazione online su attività politiche libere e regolari, come parte del processo democratico. Con l'accento sulla cooperazione più pratico, le nostre discussioni anche focalizzati su temi quali:

- l'inquadratura ingannevole di una libera offerta come pratica sleale;
- l'opportunità di adottare rimedi strutturali in grado di provocare un cambiamento nei modelli di business attuali;
- regolazione asimmetrica dei dati di accesso;
- l'uso improprio della protezione dei dati da parte delle autorità nazionali, comprese le agenzie di concorrenza, a frustrare le indagini.

Le autorità hanno anche discusso fattori non di prezzo nell'analisi della concorrenza e l'applicazione dei consumatori e hanno convenuto di proseguire discussioni parallele su questo, per sviluppare una metodologia per valutare i costi reali per gli individui, quando il costo monetario di un servizio è pari a zero o al di sotto del costo marginale.

Andando avanti, ci proponiamo di continuare i nostri sforzi all'interno della stanza di compensazione digitale per garantire la coerenza delle aree di indagine già in discussione, mentre anche cercando di contribuire e costruire sul lavoro delle reti esistenti.



@EU\_EDPS

Il **#DigitalClearinghouse** incontrato per la quarta volta ieri. 31 autorità da **#UNIONE EUROPEA** e in tutto il mondo discusso le sfide comuni nel

**# digitale** ecosistema. Leggi la dichiarazione adottata dalla rete [https:// europa. eu /! NY93Mq](https://europa.eu/!NY93Mq)

#### 4.5. AFFARI INTERNAZIONALI

Nell'era digitale in cui stiamo vivendo, tutti e tutto è collegato, indipendentemente da dove siamo nel mondo. Tuttavia, mentre i dati personali ora fluisce liberamente attraverso i confini, leggi sulla protezione dei dati rimangono nazionale o, nel migliore dei casi, regionale.

Meglio l'impegno e la convergenza in materia di protezione dei dati a livello internazionale, è stato oggetto di intense discussioni per molti anni e l'Europa ha assunto una posizione di leadership nel plasmare uno standard globale, digitale per la privacy e la protezione dei dati. Tuttavia, fino a tempi più recenti, era stato fatto pochi progressi pratici.

Nostro [strategia 2015-2019](#) posiziona il GEPD in prima linea in questa discussione. All'inizio del presente mandato ci siamo impegnati a forgiare partnership globale con l'obiettivo di costruire un consenso sociale globale sui principi relativi alla protezione dei dati.

Un modo in cui abbiamo cercato di raggiungere questo obiettivo è attraverso il lavoro con i nostri partner internazionali e regionali per la protezione dei dati tradizionale negli accordi internazionali. Il nostro lavoro con il Consiglio d'Europa e le organizzazioni internazionali è un buon esempio di questo, come lo sono i nostri sforzi per garantire che gli accordi dell'UE sui trasferimenti internazionali di dati, come ad esempio la Privacy Shield, rispettino pienamente i diritti fondamentali dell'UE.

#### 4.5.1 trasferimenti di dati internazionali

##### La Privacy UE-USA Shield

La Privacy UE-USA Shield è in vigore dal 1 ° agosto 2016. Si tratta di ciò che è noto come un *decisione di adeguatezza*, che prevede una base giuridica per il trasferimento dei dati personali dall'UE agli Stati Uniti. La Privacy Shield è rivista su base annuale, al fine di garantire che sia implementata in modo efficace, in modo da fornire una adeguata protezione dei dati personali, in linea con le norme UE.

La seconda revisione annuale del UE-USA Privacy Shield ha avuto luogo il 18 e 19 ottobre 2018. Un gruppo di rappresentanti dell'UE [autorità per la protezione dei dati](#)

(DPA), tra cui un rappresentante del GEPD, hanno preso parte alla rassegna. Una relazione sui risultati di questa revisione congiunta deve essere adottata al gennaio 2019 Riunione plenaria del Comitato europeo per la protezione dei dati (EDPB).



##### Una decisione di adeguatezza per il Giappone

Nel mese di settembre 2018, la Commissione Europea ha pubblicato un progetto di decisione di adeguatezza per il trasferimento dei dati personali dall'UE al Giappone. Prima di adottare la decisione, la Commissione era tenuta a consultare l'EDPB di parere.

L'EDPB ha adottato questo parere il 5 dicembre 2018, utilizzando il suo documento di orientamento aggiornato sulle decisioni di adeguatezza come un punto di riferimento. Come la prima decisione sull'adeguatezza dell'era GDPR, la decisione sull'adeguatezza UE-Giappone non solo impostare il tono per eventuali decisioni di adeguatezza future, ma può anche avere un impatto sulla prossima revisione di tutte le decisioni di adeguatezza attualmente in vigore.

La Commissione ha inoltre consultato il GEPD e, il 4 settembre 2018, abbiamo formulato osservazioni informali preliminari sul progetto di decisione. Tuttavia, in contrasto con il nostro approccio al progetto UE-USA Privacy Shield nel 2016, non abbiamo espresso un parere. Questo perché, in quanto membro della EDPB, abbiamo contribuito attivamente alle discussioni sul parere EDPB, disegno particolare attenzione al ruolo del consiglio e la responsabilità della Commissione per le decisioni di adeguatezza. Convinti che il parere EDPB rappresentava una ragionevole riflessione discussioni consiliari, abbiamo incoraggiato la Commissione a prendere le sue osservazioni e raccomandazioni in considerazione.



@EU\_EDPS

Lieto [#EDPS](#) ha fortemente contribuito ad una equilibrata [@EU\\_EDPB](#) parere di fondamentale importanza al primo

[#GDPR](#) accertamento di adeguatezza: Non light rosso, ma

miglioramenti

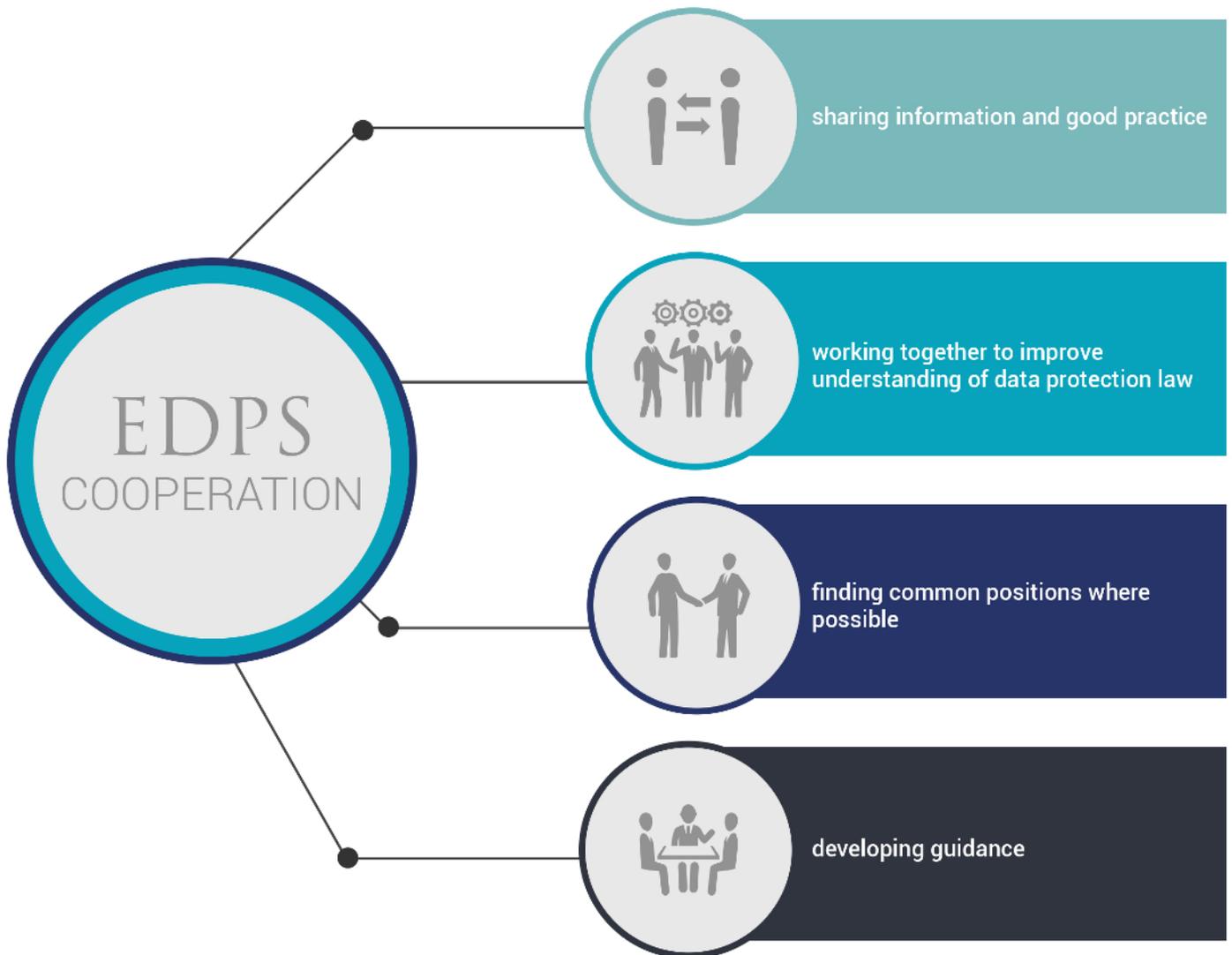
consigliata per ottenere un robusto

[#UNIONE EUROPEA](#) & [#Giappone](#) [#protezione dati](#) affare

#### 4.5.2 Cooperazione internazionale

##### Consiglio d'Europa

La Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati personali è lo strumento internazionale giuridicamente vincolante prima nel campo della protezione dei dati. Adottata dal Consiglio d'Europa il 28 gennaio 1981, ogni paese può iscriversi a ciò che è noto come Convenzione 108.



53 paesi sono ormai parte della Convenzione e il suo Protocollo aggiuntivo concernente le autorità di controllo e i flussi transfrontalieri di dati. Questi includono Capo Verde e il Messico, dove la convenzione è entrata in vigore il 1 ° ottobre 2018. In combinazione con il numero dei paesi che partecipano al Comitato della Convenzione 108 in qualità di osservatori, questo numero aumenta a 70 paesi, lavorando tutti insieme in materia di privacy e protezione dei dati diritti.

Il ruolo del GEPD, in quanto istituzione dell'Unione europea, è di agire in qualità di osservatore nel Consiglio dei gruppi di esperti europei in materia di protezione dei dati. Questi gruppi comprendono il Comitato consultivo (T-PD) della Convenzione 108. Partecipiamo alle riunioni dei gruppi di esperti e fornire commenti, al fine di garantire sia un alto livello di protezione dei dati e la compatibilità con gli standard di protezione dei dati dell'UE.

Da qualche tempo, il Consiglio d'Europa ha lavorato per modernizzare Convenzione 108. L'obiettivo era quello di rafforzare l'efficacia e assicurarsi che meglio riflette la realtà di un mondo sempre più connesso. Il GEPD ha seguito questo processo in tutto.

Il 18 maggio 2018, è stato adottato il Protocollo che modifica la Convenzione. Riafferma i principi essenziali sanciti dalla Convenzione di testo originale e integra nuove garanzie. Conosciuto come **Convenzione 108+**, **La nuova convenzione modernizzato 108** è stata aperta alla firma il 10 ottobre 2018 e firmato da 21 stati in una cerimonia ufficiale.

Nel 2018, abbiamo contribuito a discussioni del T-PD su una raccomandazione sui dati relativi alla salute, lavori in corso sul meccanismo di follow-up della convenzione 108+, Intelligenza Artificiale (AI), la Corporation Internet

Assigned Names e Numbers (ICANN) e l'applicazione della legge l'accesso transfrontaliero ai dati.

### Organizzazioni internazionali

Anche se possono essere esenti da leggi nazionali, comprese quelle relative alla protezione dei dati, le organizzazioni internazionali sono sostenitori influenti per lo sviluppo di una cultura della privacy. La loro posizione significa che sono in grado di diffondere la conoscenza sulla protezione dei dati e della privacy in alcune parti del mondo in cui, per vari motivi, non è stato necessariamente all'ordine del giorno.

Sosteniamo le organizzazioni internazionali nei loro sforzi per sviluppare le proprie strutture di protezione dei dati e di condividere conoscenze ed esperienze con l'un l'altro. Una parte importante di questo lavoro si svolge nel quadro di una serie di workshop, iniziativa abbiamo lanciato nel 2005.

Nel mese di luglio 2018, garante Wojciech Wiewiórowski partecipato alla settima edizione di questi laboratori, che abbiamo avuto il piacere di co-organizzazione di Copenhagen a fianco dei nostri padroni di casa, l'Ufficio dell'Alto Commissario delle Nazioni Unite per i rifugiati.

Il workshop si è concentrato su una serie di argomenti. Tra questi:

- standard di privacy e meccanismi di controllo per le organizzazioni internazionali;
- come mettere il principio della responsabilità in pratica;
- trasferimenti internazionali;
- le basi giuridiche per il trattamento dei dati personali nel contesto internazionale organizzazioni.

Durante le nostre discussioni abbiamo notato una comune determinazione a far parte di protezione dei dati della cultura del lavoro delle organizzazioni internazionali e di garantire che queste organizzazioni sono ritenuti responsabili. Non abbiamo alcun dubbio sul fatto che i dialoghi produttive avviate a questo workshop porterà a ulteriori collaborazioni tra le stesse organizzazioni internazionali che continuano a sviluppare le loro approcci alla protezione dei dati. Il GEPD presterà il nostro pieno sostegno a questo sforzo.

### Il Gruppo di Berlino

Il GEPD è stato un membro attivo del gruppo internazionale di lavoro sulla protezione dei dati e delle telecomunicazioni (IWGDPT, noto come il Gruppo di Berlino) sin dalla sua istituzione. Il lavoro del gruppo è

diventando sempre più importante con la crescente enfasi posta sul ruolo della tecnologia e il suo impatto sui diritti fondamentali, così come il riconoscimento giuridico della protezione dei dati in base alla progettazione come un obbligo per i controllori.

Come un organismo di cooperazione globale, l'IWGDPT riunisce attori provenienti da diverse parti del mondo, non solo da entrambi i lati dell'Atlantico, ma anche dal di là del Pacifico. Tutti hanno diversi punti di vista e approcci per i diritti degli individui e dei modelli per la loro protezione. Trovare una posizione comune conciliare i vari ambiti di provenienza può essere impegnativo, ma questo rende i risultati ancora più potente e utile.

IWGDPT Working Papers si basano su un'analisi delle caratteristiche tecnologiche coinvolte nel soggetto della carta. Allora continuano ad principi ine e raccomandazioni volte a raggiungere obiettivi comuni. Nel 2018, Working Papers riguarda l'elaborazione dei dati e la raccolta di veicoli collegati. Il gruppo ha lavorato anche sulle sfide alla privacy di Intelligenza Artificiale.

### II-Ibero Americano Conference

La Conferenza iberoamericana XVI in materia di protezione dei dati ha avuto luogo dal 28-30 novembre 2018, a San Jose, Costa Rica. Abbiamo avuto il privilegio di partecipare alla conferenza, che ha riunito i rappresentanti del Sud e del Centro America DPA, le grandi aziende e la società civile.

Tra gli argomenti discussi sono stati le relazioni tra l'UE e l'America latina, la protezione dei dati personali dei minori, nuove prospettive nel trattamento dei dati sanitari, la sicurezza contro la privacy e il ruolo della società civile nella tutela dei dati personali. Il GEPD ha contribuito al pannello sulla trasparenza e la protezione dei dati.

Una sessione a porte chiuse ha avuto luogo l'ultimo giorno, permettendo alle autorità dei paesi partecipanti per fornire un l'altro con un aggiornamento sulla loro legislazione in materia di protezione dei dati, compresi gli emendamenti, la firma di convenzioni internazionali e la stesura di una nuova legislazione. La conferenza è stata un'ottima occasione per noi per sviluppare i rapporti con i nostri omologhi in America Latina.

## 4.6 DIGITALE ETICA

Nel corso degli ultimi due decenni, abbiamo assistito a una rivoluzione digitale che ha cambiato il nostro mondo in modi che erano inimmaginabili. Mentre numerosi sviluppi hanno portato benefici, abbiamo anche bisogno di confrontarsi con una serie di nuovi problemi e sfide. Molti di questi sono

legata al modo in cui i dati sono raccolti e utilizzati nell'era delle tecnologie digitali. Per far fronte a questa nuova realtà, ci siamo impegnati a sviluppare una dimensione etica alla protezione dei dati in nostro [strategia 2015-2019](#).

Il nostro lavoro su etica inizia con la questione di come i valori e dei diritti fondamentali possono essere accolti nell'era digitale e mira a promuovere la conoscenza e la comprensione dei rischi che abbiamo di fronte. Vogliamo valutare come la protezione dei dati e la privacy sono legati a preservare la dignità umana nel mondo digitalizzato ed esplorare il significato e l'importanza, tenuto conto monitoraggio estensivo e profiling, l'Internet delle cose, big data, Intelligenza Artificiale (AI) e autonoma sistemi, robotica e la biometria.

L'etica è su come definire giusto e sbagliato, sia in teoria che in pratica, in circostanze specifiche. Anche se non è un'alternativa alla legge, informa le leggi in quanto sono in corso di elaborazione, interpretati e rivisti. Può anche aiutare le persone e le organizzazioni di guida nel decidere se agire o meno in una zona dove la legge sembra essere in silenzio. Il [GEPD Ethics Initiative](#) mira a raggiungere oltre la comunità immediata dei funzionari dell'Unione europea, avvocati e specialisti IT e generare una conversazione globale su questo.

2018 è stato un anno cruciale per l'iniziativa etica. L'anno è iniziato con la pubblicazione del [Rapporto Etico Advisory Group](#) e si è conclusa con una settimana di discussione intensa e produttiva durante la [2018 Conferenza internazionale di protezione dei dati e della privacy](#). Dopo più di tre anni di duro lavoro, l'etica digitali è ora molto nell'agenda globale. È fondamentale che noi ora lavoriamo per capitalizzare su questo e spostare il dibattito in avanti.

#### 4.6.1 Il gruppo consultivo etico: Segnalazione di etica Digital

Il [Advisory Group Etica \(EAG\)](#) è stato lanciato dal GEPD ai computer annuali, Privacy e protezione dei dati (CPDP) conferenza nel mese di gennaio 2016, come parte della Etica Initiative GEPD. Costituito da sei esperti di diversa formazione, il suo compito era quello di esplorare le relazioni tra i diritti umani, la tecnologia, i mercati e modelli di business nel XXI secolo.

Nel corso di due anni, il gruppo ha lavorato insieme per esaminare l'etica digitali da una varietà di prospettive di studio e professionali, con l'obiettivo di contribuire al dibattito più ampio sul ambiente digitale e le sue implicazioni etiche.

L'EAG restituito alla conferenza CPDP nel 2018, come parte di un panel organizzato dal GEPD, per presentare il loro [rapporto finale](#) e discutere le questioni sollevate all'interno di esso. Il rapporto incentrato sulle conseguenze del digitale

rivoluzione e l'impatto che queste conseguenze hanno avuto sui valori che noi, come individui e come società, di più caro. Esso ha individuato i principali cambiamenti socio-culturali che hanno avuto luogo in tandem con gli ultimi sviluppi tecnologici, esaminare la relazione tra di loro, i valori umani e agenzia etica, e si rivolse perché questo richiede una nuova valutazione dell'ecosistema protezione dei dati.

L'obiettivo della relazione non era di produrre risposte definitive o articolare nuove norme, ma per incoraggiare la riflessione proattiva su ciò che è in gioco.



#### 4.6.2 Ottenere le vostre opinioni su Etica Digitale

Il 15 giugno 2018, abbiamo lanciato una consultazione pubblica sull'etica digitali. L'obiettivo della consultazione è stato quello di costruire sui risultati del rapporto EAG, aprendo il dibattito a contributi provenienti da individui e organizzazioni in tutti i settori della società. In particolare, abbiamo voluto capire meglio come sono stati influenzati dal passaggio a, le sfide specifiche digitali di avere di fronte e in che misura sono stati affrontare queste sfide con un approccio etico-based.

Abbiamo ricevuto 76 risposte alla consultazione, da un'ampia varietà di sorgenti situate in tutto il mondo. Tra questi centri sanitari, asili, università, governi, ONG, studi legali e gli sviluppatori di software, tra gli altri. La consultazione era costituito da 12 domande, la maggior parte delle quali invitati risposte aperte, che ci permette di raccogliere informazioni qualitative di vitale importanza. Da queste risposte siamo stati in grado di raggiungere una conclusione principale: l'etica era all'ordine del giorno della maggior parte delle organizzazioni che hanno partecipato alla consultazione e sono stati considerati estremamente rilevante.



Hanno contribuito citati esempi di alcune delle sfide che abbiamo di fronte e dobbiamo affrontare. Questi robot inclusi nel settore sanitario e assistenti digitali personali, voto on-line, dando una gomitata stato e il futuro del lavoro. Uno dei partecipanti ha commentato che *privacy va oltre il rispetto, la padronanza della sfida privacy consente opportunità digitali sostenibili*. Un altro sottolineato l'importanza di

*i diritti umani e dei valori europei di libertà, uguaglianza, la libertà, la democrazia, mentre un terzo ha riconosciuto che le sfide sono immense e difficile.*

I risultati della consultazione sono stati pubblicati il 25 Settembre 2018 come parte di un [breve riassunto](#) .

#### 4.6.3 incoraggiando il dibattito in tutto il mondo

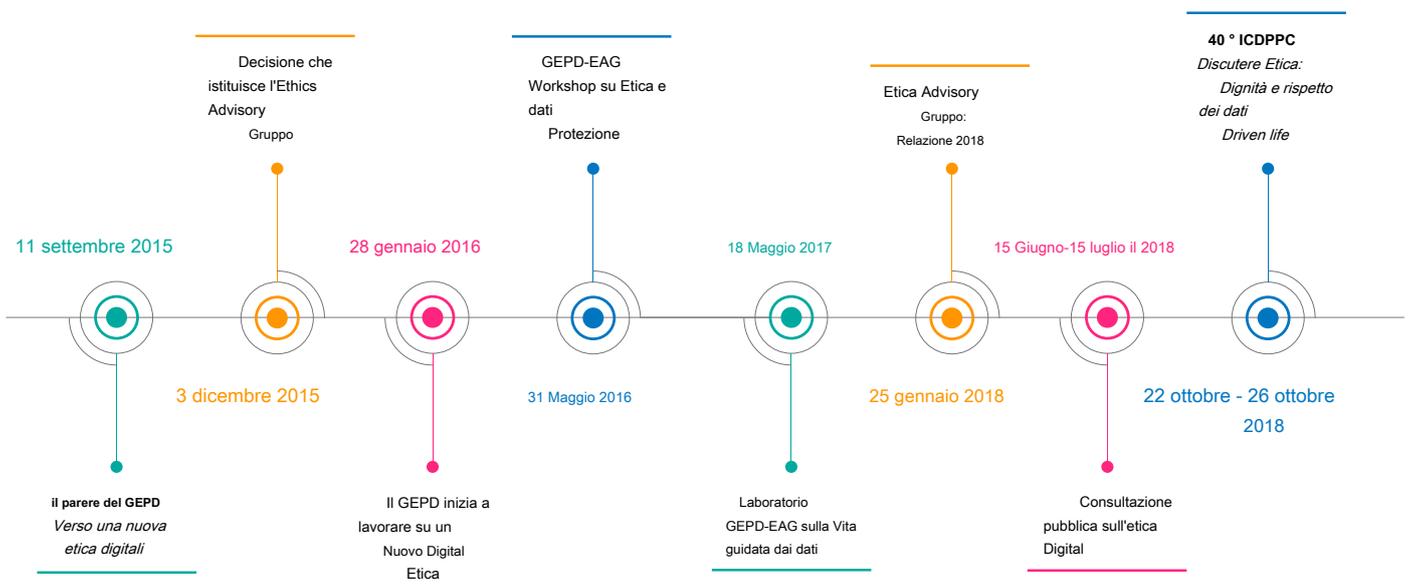
Dal 22-25 ottobre 2018, più di 1000 persone, che rappresentano una vasta gamma di discipline, nazionalità e punti di vista, scese sulla Parlamento europeo a Bruxelles per discutere di etica digitali ( [vedere paragrafo 4.7](#) ). La Conferenza Internazionale 40 ° di protezione dei dati e della privacy ha dimostrato di essere un momento di svolta per il dibattito sull'etica digitali, sulla base del lavoro prodotto attraverso l'Ethics Initiative GEPD per incitare una reazione globale alle sfide che abbiamo di fronte nell'era digitale.

Mentre le nuove leggi, come la GDPR, ci forniscono un quadro globale per la protezione dei dati nell'era digitale, sono solo un primo passo per garantire che siamo in grado di raccogliere il benef sua di fered dalle nuove tecnologie, pur godendo il nostro diritti fondamentali.

Abbiamo dedicato la conferenza *Debating Etica: Dignità e rispetto in Data Driven Life*. deliberazione etica è il processo di auto-riflessione sociale, su cui i membri di una società stabiliscono valori e norme e mettono in scena sistemi giuridici. In poche parole, l'etica vengono prima, durante e dopo la legge, che ci aiuta a garantire che le nostre leggi rimangono fino ad oggi. La storia ha dimostrato che le nozioni etiche del bene e del male deve essere discussa e definita su base continua, per mezzo di una discussione aperta e democratica. Etica, quindi,

### L'iniziativa GEPD Ethics:

#### Tre anni di lavoro



ci può aiutare a trovare una via verso un futuro sempre più digitale che sia riafferma e protegge i diritti e i valori di lunga data.

Le sfide poste dalla rivoluzione digitale richiede una risposta globale. Attraverso la conferenza, siamo stati in grado di generare il ricco dibattito globale e interdisciplinare che può ispirare questo. Sono intervenuti ad alto livello rappresentanti dell'UE, accademici rinomati, pionieri del mondo online, refusenik, attivisti, difensori dei diritti umani e rappresentanti delle ONG, nella Silicon Valley vip, esperti legali, scrittori e giornalisti, pensatori e sognatori e, naturalmente, i rappresentanti di dati autorità per la protezione di tutto il mondo.

Attraverso i nostri sforzi di comunicazione, le diverse questioni sollevate durante la conferenza ha raggiunto un numero enorme di persone, sensibilizzazione e innescando la reazione in tutto il mondo. Con almeno 1500 articoli on-line pubblicati durante la settimana della conferenza, oltre ad altri copertura mediatica, siamo stati in grado di raggiungere ben oltre le 1400 persone che hanno partecipato alla conferenza. Questo senza dubbio ci ha aiutato a mobilitare una vasta gamma di persone, al di là della comunità di protezione dei dati e al di là dell'Europa, e di fare grandi passi avanti verso il nostro obiettivo comune di sviluppare una dimensione etica alla protezione dei dati.

UN [rapporto completo](#) sui risultati della conferenza è disponibile sul sito web del GEPD ( [vedere paragrafo 4.7](#) ). In aggiunta a questo, come parte del nostro lavoro continua alla Ethics Initiative GEPD produrremo un nuovo GEPD Etica conclusioni nel 2019.

## 4.7 2018 CONFERENZA INTERNAZIONALE DI PROTEZIONE DEI DATI E COMMISSARI PRIVACY

Nel 2018, il GEPD ha avuto il privilegio di ospitare la 40 ° Conferenza internazionale di protezione dei dati e della privacy, a fianco dei nostri co-patroni di casa, la bulgara Commissione per la protezione dei dati personali (CPDP). Questa è stata la prima volta che questo conferenza annuale, che si è svolto dal 22-26 Ottobre 2018, era stato in possesso di un'istituzione dell'Unione europea, in collaborazione con l'autorità nazionale di vigilanza.

La conferenza è iniziata con una sessione chiusa due giorni, aperto solo alla conferenza membri accreditati. Abbiamo quindi accolto i partecipanti provenienti da tutto il mondo per la sessione pubblica della Conferenza. Tra i partecipanti rappresentanti del governo, della società civile, le autorità di regolamentazione, l'industria, mondo accademico e dei media, in

dipendenza da [autorità per la protezione dei dati](#) (DPA). Quaranta eventi collaterali su una vasta gamma di questioni attinenti alla privacy anche avuto luogo e gli eventi privacy supplementari sono stati organizzati anche dal nostro co-conduttore a Sofia.

La Conferenza Internazionale 40 ° di protezione dei dati e della privacy è stato un evento diverso da qualsiasi dei suoi predecessori. Essa non si è concentrato sulla privacy o protezione dei dati o leggi specifiche, come il regolamento generale sulla protezione dei dati (GDPR), o anche su leggi in generale. Piuttosto, attraverso *Debating Etica: Dignità e rispetto nella vita guidata dai dati*, abbiamo voluto costruire sul lavoro avviato dal [GEPD Ethics Initiative](#) e stimolare una discussione onesta e informati su come dovremmo modellare l'impatto della tecnologia digitale su individui e le società. Come risultato dei nostri sforzi in questo settore, il GEPD è ora visto come una delle principali autorità sull'etica digitali.

UN [rapporto dettagliato](#) sulla conferenza sono disponibili sul sito web del GEPD.



### 4.7.1 Il Closed Session - Etica e Intelligenza Artificiale

La Conferenza internazionale di protezione dei dati e della privacy (ICDPPC) è un'organizzazione internazionale riconosciuta. Nel corso della sua storia di 40 anni, la conferenza ha incontrato ogni anno, che riunisce DPA dal livello locale, nazionale e internazionale per condividere le conoscenze e fornire supporto.

Il Comitato Esecutivo ICDPPC imposta l'ordine del giorno della sessione a porte chiuse. Nel 2018, per la prima volta, il tema centrale della sessione a porte chiuse era direttamente collegato al tema della sessione pubblica.

La sessione di chiusura della Conferenza Internazionale è aperto solo ai membri accreditati e osservatori del [ICDPPC](#). Riunire un numero record di 206 delegati provenienti da 76 paesi, che ha avuto luogo presso la

prestigioso Palais d'Egmont, a Bruxelles dal 22-23 ottobre 2018. Etica e Intelligenza Artificiale (AI) è stato argomento di discussione questi anni.

Pochi autorità attualmente controllano così strettamente e intensamente come garanti per la protezione dei dati e la privacy l'impatto delle nuove tecnologie sui diritti fondamentali. La conferenza 2018 ha proseguito la discussione su AI iniziata due anni prima in occasione della conferenza di Marrakesh, che si basava su un [documento di riflessione](#)

prodotta dal GEPD.

Le nostre discussioni hanno portato in un [dichiarazione](#) sull'etica e la protezione dei dati nel campo dell'intelligenza artificiale, che spiegano sei principi per il futuro sviluppo e l'uso di intelligenza artificiale e impegnativi sforzi internazionali concertati per attuare questi principi. membri di una conferenza contribuiranno a questi sforzi in modi diversi anche attraverso un [consultazione pubblica](#) e un nuovo gruppo di lavoro permanente per l'etica e la protezione dei dati in intelligenza artificiale.

La camera di consiglio ha inoltre adottato altre tre risoluzioni sulla [piattaforme e-learning](#), sul [censimento Conference](#) e [collaborazione tra le autorità di protezione dei dati e le autorità per la protezione dei consumatori](#), Oltre ad un [tabella di marcia per il futuro della Conferenza internazionale](#).

Ci auguriamo che le decisioni prese nella sessione chiusa aiutano la conferenza di crescere in modi che rafforzare la cooperazione a livello globale. Come comunità di regolatori, l'ICDPPC deve ora cercare di interagire molto di più con i partner al di fuori del mondo della protezione dei dati.

#### 4.7.2 Il Sessione pubblica - Debating Etica



La sessione pubblica della Conferenza internazionale del 2018 ha avuto luogo dal 24-25 Ottobre 2018, nell'emiciclo del Parlamento europeo a Bruxelles. Oltre a ospiti, membri e osservatori del ICDPPC, abbiamo

accolto i partecipanti di diversa estrazione e nazionalità. Questi rappresentanti inclusi dal settore pubblico e privato, del mondo accademico, della società civile e dei media.

Con la scelta del tema per la sessione pubblica a discrezione dei padroni di casa, abbiamo scelto di concentrarsi su *Debating Etica: Dignità e rispetto in Data Driven Life*. Abbiamo voluto ispirare un dibattito inclusivo, interdisciplinare e interattivo sulla rivoluzione digitale e il suo impatto su di noi, come individui e come società ([vedere paragrafo 4.6](#)).

Suddiviso in cinque sessioni tra due giorni, la conferenza ha attirato su contributi di un gruppo eterogeneo di altoparlanti. Questi rappresentanti compresi di alto livello UE, accademici rinomati, pionieri del mondo online, refusenik, attivisti, difensori dei diritti umani e rappresentanti delle ONG, nella Silicon Valley VIP, esperti legali, scrittori e giornalisti, pensatori e sognatori e, naturalmente, i rappresentanti di DPA da tutto il mondo.


@EU\_EDPS

**# GEPD @Buttarelli\_G** apre i Giochi Olimpici 2018 su **#Privacy** - "Scegliere l'umanità: mettere la dignità di nuovo in digi tal". Il 40° International conference esplorerà la dimensione umana delle nuove tecnologie.

**#DebatingEthics @icdppc2018**

#### Sessione uno - Questa Digital Life

La conferenza è iniziata con una discussione sul ruolo dell'etica nella società umana. Maria Farrell, uno scrittore e consulente per la tecnologia, la politica e la comunità Internet, ha iniziato la conferenza con una richiesta di azione collettiva che impostare il tono per le discussioni a venire.

GEPD e padrone di casa, Giovanni Buttarelli, ha aperto ufficialmente la conferenza, che definisce l'importanza strategica di definire un'etica digitali veramente globali che tutela la dignità e il rispetto per gli individui e gruppi nei decenni a venire. Parte integrante questa è la necessità di una valutazione obiettiva di come le tecnologie stanno influenzando la nostra vita e come possiamo garantire un rapporto positivo

con le nuove tecnologie, che mette le persone e la dignità al centro.

Ha terminato il suo discorso, accogliendo uno dei nostri relatori, Tim Cook, sul palco. In un discorso atteso molto, il CEO di Apple ha fatto una chiamata potente per lo sviluppo di un'etica digitali e ha riconosciuto la responsabilità di Apple e altri sviluppatori potenti nel garantire la tecnologia serve l'umanità.

#### Sessione due - giusto contro sbagliato

La seconda sessione sembrava di valutare come le ultime innovazioni tecnologiche impatto la nostra privacy, l'autonomia e l'autodeterminazione. Abbiamo voluto esplorare come l'etica interagisce con la legge, il ruolo che ha giocato in altri campi e il ruolo che essa svolge nella risoluzione di dilemmi di politica pubblica.

Inventore del World Wide Web Sir Tim Berners-Lee e Professore di Diritto e Filosofia presso l'Università della Pennsylvania Anita Allen apre il dibattito. Mentre il primo ha sottolineato il ruolo di sviluppo tecnologico nel plasmare la società, quest'ultima ci ha incoraggiato a vedere l'etica come qualcosa che integra la legge, piuttosto che mina esso.

Una tavola rotonda seguita, con studiosi di etica di fama e studiosi che hanno offerto spunti nell'applicazione dell'etica in diversi campi.

#### Sessione di tre - il dividendo digitale

Nell'ultima sessione della giornata, abbiamo guardato le più ampie conseguenze sociali di etica. L'obiettivo era di esplorare l'effetto delle nuove tecnologie sui valori e diritti in gioco per gli individui e l'interazione umana, della società e dello Stato

Gli amministratori delegati di due dei più grandi aziende tecnologiche al mondo, Facebook e Google, hanno contribuito alla nostra discussione attraverso messaggi video, mentre l'ex Presidente della Corte Suprema dell'India, Jagdish Singh Khehar, ci ha fornito un esempio reale di come l'etica possano essere attuate.

Dopo una tavola rotonda sull'impatto delle tecnologie sulla società e l'economia emergente, cade il nostro co-conduttore, presidente della commissione bulgara per la protezione dei dati personali Ventislav Karadjov, per riassumere discussioni della giornata.

Abbiamo finito la giornata con la chiamata di filosofia del computer scrittore Jaron Lanier per un meno manipolativo alternativa al modello di business della pubblicità che attualmente domina il settore della tecnologia.

#### Sessione quattro - Verso un'Etica Digitale

Il commissario europeo per la Giustizia vera Jourová aperto il nostro secondo giorno di discussioni, che si è concentrata sul concetto di *la protezione dei dati oltre la conformità*. Abbiamo cercato di determinare in che modo questo concetto, che dovrebbe parlarne e che ha bisogno di agire.

Una questione importante in questo dibattito riguarda il ruolo del DPA nella governance dell'etica digitali. Una tavola rotonda con garanti della privacy provenienti da ogni continente, così come ts EXPER stimati dal governo, la società civile e l'industria, ha cercato di rispondere a questa domanda.



#### Sessione cinque - Spostare più lento e sistemare le cose

La nostra sessione finale mirava a trarre conclusioni dalle discussioni precedenti, con particolare attenzione su come andare avanti. E 'incluso un rapporto sui risultati del Creative Café, una sessione di workshop in parallelo alla sessione di quattro, che si proponeva di esplorare questa domanda.

Parlando a nome del Creative Café, garante Wojciech Wiewiórowski sottolineato la che la conferenza ha rappresentato solo l'inizio di un processo molto più lungo.

GEPD Giovanni Buttarelli ha portato alla conferenza al termine. Egli fa riferimento la diversità delle voci udite durante le sessioni, da coloro che hanno rappresentato potenti interessi, a coloro che hanno parlato per i più svantaggiati, che sono ancora di beneficiare realmente dalla rivoluzione digitale.

Oltre 40 persone hanno preso sul palco durante la sessione pubblica della conferenza internazionale, offrendo loro

diversi punti di vista sul tema dell'etica digitali. Comune a tutti i loro contributi era una promessa: di continuare la collaborazione istigato dalla conferenza alla ricerca di un'etica digitali sostenibili.



#### 4.7.3 Eventi collaterali

Nella tradizione degli anni passati, eventi collaterali, ancora una volta hanno avuto luogo a margine della conferenza internazionale 2018. Questi concentrati non solo sul tema della conferenza di etica digitali, ma anche su una vasta gamma di altri argomenti relativi alla pratica di protezione dei dati. Con oltre 40 eventi tra cui scegliere, tutti che si terrà il 23 e 25 ottobre 2018, c'era qualcosa per tutti gli interessi.

Organizzato da una varietà di diverse organizzazioni e gruppi provenienti da tutto il mondo, gli eventi collaterali che hanno avuto luogo durante la settimana della settimana conferenza internazionale fornito un'opportunità unica per i partecipanti di interagire con i colleghi di diverse nazionalità e background e di imparare dai loro dif Fering prospettive su una serie di questioni relative alla protezione dei dati. La diversità degli argomenti trattati è ben illustrato da una selezione di eventi.

Nell'anno del [Il regolamento generale sulla protezione dei dati](#) (GDPR) è forse sorprendente che molti dei nostri eventi collaterali focalizzati sul tema. Il GEPD e del Consiglio sulla protezione dei dati europea (EDPB) ha ospitato congiuntamente uno di questi eventi, il 25 ottobre 2018. Gli esperti della protezione dei dati e di altre autorità in tutta l'UE e si unirono a livello globale le teste del GEPD e EDPB, Giovanni Buttarelli e Andrea Jelinek, per un discussione sulla GDPR, cinque mesi dopo che è diventato pienamente applicabile. L'evento è stato onorato di accogliere Koen Lenaerts, presidente della Corte di giustizia dell'Unione europea, Catherine De Bolle, direttore esecutivo di Europol, come i suoi relatori.

Un altro evento, organizzato dal Consiglio d'Europa, ha visto una linea impressionante di esperti di protezione dei dati discutere le loro opinioni sulla modernizzazione della Convenzione 108, unico trattato internazionale del mondo salvaguardia del diritto alla [protezione dei dati](#) (vedere la sezione 4.5.2). L'evento mirava a decomprimere il recentemente aggiornato convenzione

108, che fornisce informazioni sul nuovo testo, il suo valore e benefici.

Public Voice Coalition, un'ampia coalizione di organizzazioni della società civile, ha organizzato un altro evento, incentrato su uno dei temi caldi in materia di protezione dei dati al momento: Intelligenza Artificiale. Con evidenti collegamenti con l'etica digitali, l'evento sembrava di esplorare le implicazioni di intelligenza artificiale per i diritti umani, la tutela dei consumatori e della concorrenza e il rapporto tra l'etica e la legge.

Eventi collaterali sono stati organizzati da otto diversi DPA da tutto il mondo, 18 ONG e organizzazioni internazionali, sei think tank e gruppi di ricerca e otto aziende private e studi legali. Oltre 160 altoparlanti sono stati coinvolti in quello che si è rivelata una selezione molto varia di eventi.


@EU\_EDPS

Più di 200 delegati provenienti da [#DPAs](#) rappresentati alla 40 ° Conferenza Internazionale di [#Protezione dati](#) & [#Privacy](#) Commissari a Bruxelles. Caloroso ringraziamento a più di 1400 delegati, relatori, partecipanti per proficue discussioni e ambiente stimolante!

[#DebatingEthics](#) [#icdppc2018](#)

#### 4.7.4 Eventi sociali

Al fine di offrire un'esperienza unica per i delegati provenienti a Bruxelles da tutto il mondo, abbiamo ottenuto alcuni dei luoghi più suggestivi e prestigiosi di Bruxelles di ospitare la conferenza. Abbiamo voluto dare delegati un assaggio di ciò che il *Capitale d'Europa* ha da offrire, compresa la sua storia e l'architettura impressionante.

La settimana è iniziata a Bruxelles Hôtel de Ville, un imponente edificio gotico risalente al XV secolo. I delegati di oltre 80 paesi sono stati accolti con un cocktail di benvenuto e una vista spettacolare della piazza centrale di Bruxelles, il Grand Place.

Da Ottobre 22-23 2018, ICDPPC accreditati i membri e gli osservatori sono riuniti presso il Palais d'Egmont, la sede per la sessione a porte chiuse del convegno. Originariamente costruito nel XVI secolo, il Palais d'Egmont ha ospitato diversi membri della regalità e nobiltà europea nel corso degli anni, tra cui la regina

Cristina di Svezia e Luigi XV, nonché di filosofi europei di spicco e artisti, come Voltaire e Jean-Baptiste Rousseau. Ora di proprietà del Ministero degli Affari Esteri del Belgio, ospita una serie di importanti eventi diplomatici e ha accolto alcuni dei capi più influenti e conosciute al mondo di Stato.

La sede per la sessione pubblica era ugualmente impressionante. L'Emiciclo del Parlamento europeo ospita solitamente il più grande parlamento transnazionale del mondo. Dal 24-25 ottobre 2018, tuttavia, ha ospitato un dibattito tra oltre 1000 persone sull'impatto della rivoluzione digitale.

Eventi serali sono stati programmati con la stessa attenzione ai dettagli. Il primo giorno di discussioni in sede di consiglio si è conclusa con la cena presso il Concert Noble. Questo maniero storico fu costruita dal re Leopoldo II nel XIX secolo per fornire una cornice adeguata per le riunioni di socialites aristocratiche di godere la musica e l'arte.

Un cocktail di benvenuto è stato organizzato il 23 ottobre 2018 presso il Museo di Belle Arti di ispirazione, a Bruxelles Place Royale. Il tema per l'evento è stato *Una serata a Bruxelles ed è stato organizzato dai padroni di casa conferenza in collaborazione con l'International Association of Privacy Professionals (IAPP)*. Che si svolgono alla vigilia della seduta pubblica, ha incluso un tour delle opere del famoso pittore surrealista René Magritte, così come la possibilità di assaggiare alcune birre tipiche del Belgio da birrerie locali e il cioccolato belga di fama mondiale.

A seguito di una intensa prima giornata di dibattito sull'etica digitali, abbiamo organizzato la tradizionale cena di gala, che ha avuto luogo presso lo spettacolare museo Autoworld. Il museo è sede di una delle più grandi collezioni di veicoli in tutto il mondo e l'evento si è rivelato un'ottima opportunità per il networking.

Poiché nessuna visita a Bruxelles è completo senza una visita alla Atomium, l'evento finale della settimana è stata organizzata in questo museo a forma di atomo, in collaborazione con fflow e Qwant. Questo punto di riferimento di Bruxelles è stato originariamente costruito per il World Expo 1958 a Bruxelles.



## Comunicazione 4.7.5 Conference

incoraggiando il dibattito sull'etica digitali in tutto il mondo è uno degli **obiettivi principali dell'iniziativa etica, come indicato nella strategia GEPD (vedere la sezione 4.6.3)**. Con questo in mente, abbiamo messo in atto una strategia mediatica globale intesa a garantire un'ampia copertura internazionale della Conferenza, che avrebbe incitato dibattito globale.

Abbiamo anche voluto assicurare la partecipazione di tutti i partecipanti alla conferenza. Abbiamo quindi invitato tutti i partecipanti di essere coinvolti nella discussione convegno, in particolare tramite la nostra applicazione conferenza.

### campagna mediatica

Ottantuno organizzazioni dei media provenienti da 23 diversi paesi e tutti i continenti hanno seguito l'evento di quattro giorni, per un totale di 125 giornalisti. Le emittenti, agenzie di stampa e giornali importanti erano tutti presenti, compresi i mezzi di comunicazione come la CNN, CNBC, Bloomberg, il Wall Street Journal e il Financial Times. Mentre le nazioni più rappresentate sono state altamente Belgio, Stati Uniti, Italia e nel Regno Unito, abbiamo anche accolto giornalisti provenienti da Giappone, Cina, Emirati Arabi Uniti, Senegal, Kenya e altrove. Rassegna stampa della conferenza è stato veramente di portata globale.

Questa presenza media internazionali riflette interesse globale sia l'argomento di discussione e gli altoparlanti coinvolti. discorsi programmatici da CEO di Apple Tim Cook e inventore del World Wide Web Sir Tim Berners-Lee senza dubbio contribuito a premere l'interesse alla conferenza e ha contribuito a diffondere il nostro messaggio ad un pubblico più vasto.

Il 24 ottobre 2018, il primo giorno della sessione pubblica, abbiamo organizzato una conferenza stampa. Tenuto al Parlamento europeo, ha presentato i professionisti dei media, con l'opportunità di affrontare direttamente alcuni dei nostri oratori, tra cui GEPD Giovanni Buttarelli, Sir Tim Berners Lee e UK Information Commissioner Elizabeth Denham, tra gli altri. Abbiamo anche pubblicato un comunicato stampa.

Rassegna stampa della conferenza ben superato le nostre aspettative, con oltre 1500 articoli online pubblicati tra il 22 e il 26 ottobre 2018.

### Il sitoweb

#### Un dedicato sito web per la conferenza internazionale

è stato lanciato il 19 marzo 2018. Il nostro obiettivo era quello di creare un sito web user-friendly in cui la gente potrebbe facilmente trovare ulteriori informazioni sul tema della conferenza, il programma, gli altoparlanti e locali. Ha fornito

per la registrazione conferenze e partecipanti offerto la possibilità di prenotare un hotel tramite il sito e contattaci se avevano domande. I membri ICDPPC avevano anche l'accesso a tutti i documenti di riunione utilizzando i propri dati di login e password.

Il sito è disponibile in due lingue, inglese e francese, ed è stato aggiornato regolarmente in entrambe le lingue. I commenti ricevuti sul sito è stata molto positiva e ha indicato che le persone erano facilmente in grado di trovare le informazioni di cui avevano bisogno.

Nel corso della conferenza, abbiamo cercato di mantenere il sito sempre aggiornato caricando prontamente documenti, video e notizie non appena erano disponibili per noi.



### I social media

Per incoraggiare i partecipanti e gli altri a essere coinvolti nel più ampio dibattito in linea sia prima che durante la conferenza, abbiamo lanciato dedicato [cinguettio](#) e [Instagram](#) conti. Siamo stati attivi su entrambi questi

canali, fornendo aggiornamenti regolari, le informazioni e la copertura della conferenza. Abbiamo sostenuto le nostre attività su questi canali **utilizzando gli account di social media (GEPD vedere la sezione 7.1.1)**.

Abbiamo inviato un tweet 128 volte e i nostri seguaci raddoppiato nel corso della settimana della conferenza. I nostri post sono stati retweeted più di 1100 volte e ha ricevuto 1400 calibro. Su Instagram, abbiamo pubblicato 46 volte e ha ricevuto 856 calibro.

In parallelo, la visibilità del GEPD Twitter, account LinkedIn e YouTube aumentato a seguito dei nostri sforzi nel corso della conferenza, che ci permette di raggiungere nuove persone e di aumentare in modo significativo l'impatto dei nostri account di social media.

Il nostro successo sui social media dimostra sia la nostra crescente influenza globale come un'autorità in materia di protezione dei dati e l'etica digitali e la nostra capacità di raggiungere un pubblico più ampio.

### L'applicazione

Per incoraggiare la partecipazione del pubblico alla conferenza, abbiamo sviluppato e lanciato un'applicazione convegno gratuito, che era disponibile per il download dal 3 ottobre 2018. L'applicazione riflessa e completato il sito web. Tutti i delegati sono stati invitati a scaricare il programma per l'utilizzo durante la sessione pubblica della conferenza internazionale 2018.

I partecipanti possono utilizzare l'applicazione per prendere appunti, partecipare a sondaggi, condividere le loro opinioni e inviare le domande per l'host per gli altoparlanti per rispondere sul palco. 965 persone hanno scaricato l'applicazione e più del 50% collegato al proprio account personale.

## 5. Casi giudiziari



Il GEPD possono essere coinvolti in cause dinanzi alla Corte di giustizia dell'Unione europea (CGUE) in uno dei tre modi:

- il GEPD può adire la Corte;
- le decisioni del GEPD possono essere impugnate dinanzi alla Corte;
- il GEPD può intervenire nei casi rilevanti per i nostri compiti.

Abbiamo seguito da vicino tutti i casi giudiziari in materia di protezione dei dati personali nel 2018, anche se non siamo stati coinvolti direttamente in qualsiasi noi stessi. Le sentenze effettuate su casi relativi alla protezione dei dati ci aiutano ad interpretare il diritto alla protezione dei dati e per garantire che il diritto fondamentale alla vita privata e alla protezione dei dati è pienamente rispettata.

## 6. Trasparenza e Accesso Documenti



Come istituzione dell'UE e secondo le nostre regole di procedura, il GEPD è soggetto al regolamento 1049/2001, relativo all'accesso del pubblico ai documenti. Entro il GEPD, il responsabile per la gestione di queste richieste è un ufficiale legale designato. Nel loro ruolo di

Trasparenza Ufficiale, collaborano con i membri del personale interessati al fine di rispondere in modo adeguato alla richiesta.

Nel 2018, abbiamo ricevuto solo nove richieste di accesso del pubblico per i documenti detenuti dal GEPD, in confronto alle 11 richieste che abbiamo ricevuto nel 2017. Il calo riflette il trend degli ultimi anni. Di queste richieste, un caso è stato esaminato in una fase di conferma. In tutti i casi i documenti richiesti sono stati completamente o parzialmente divulgato.

Sembra che la diminuzione del numero di richieste ricevute è il risultato dei nostri sforzi proattivi per aggiornare e pubblicare le informazioni sul nostro sito web in modo semplice e accessibile regolarmente. Rimaniamo pienamente impegnati ad aumentare la trasparenza e la responsabilità del nostro lavoro e proponiamo di aggiornare il nostro sito web, e la nostra [registro pubblico](#) in particolare, con i documenti e le informazioni su base regolare rilevanti.

## 7. L S EGRETARIATO

### 7.1 INFORMAZIONE E COMUNICAZIONE

Come il profilo della protezione dei dati continua a crescere, è il lavoro del GEPD informazione e comunicazione di squadra per garantire che i nostri messaggi e le attività riflettono e sostenere la reputazione del GEPD come una delle principali autorità in questo settore. Questo ruolo è di cui il GEPD

**strategia 2015-2019**, Che impegna le GEPD di rendere problemi tecnici più accessibile per i non esperti e comunicare in modo trasparente, appropriato per il pubblico pertinenti.

2018 è stato un t ticola re par LY anno molto impegnativo per il team di comunicazione, e il GEPD in generale. I preparativi per il Consiglio europeo di protezione dei dati (EDPB) e la **II regolamento generale sulla protezione dei dati** (GDPR) è venuto al culmine nel maggio 2018, mentre abbiamo anche lanciato ed eseguito campagne di comunicazione sulla **2018 Conferenza internazionale di protezione dei dati e della privacy** (vedere la sezione 4.7.5) E le nuove regole sulla protezione dei dati per le istituzioni e gli organi dell'UE.

Oltre a queste attività, abbiamo continuato i nostri sforzi per migliorare i nostri canali di comunicazione stabiliti, basandosi sul successo degli sforzi di rebranding nel corso degli ultimi anni per rafforzare l'immagine del GEPD come leader globale rispettato nel settore della protezione dei dati.

#### 7.1.1 dei media online



#### Sito web

**Dal lancio del nostro nuovo sito web nel 2017, abbiamo continuato a migliorare con l'aggiunta di nuove funzionalità e migliorare il design.** Questi sforzi sono volti a fornire la migliore esperienza utente possibile e garantire che tutti i visitatori del sito sono facilmente in grado di trovare le informazioni di cui hanno bisogno.

Uno dei miglioramenti che abbiamo introdotto nel 2018 è stato quello di **aggiungere un Link veloci sezione per la home page per fornire agli utenti un collegamento ad alcune delle pagine più frequentemente utilizzate sul nostro sito.** Dove possibile, abbiamo anche spostato dalla pubblicazione di documenti in formato PDF per la loro produzione in HTML, garantendo una migliore esperienza utente sui telefoni cellulari e tablet. Nell'interesse della trasparenza, ci assicuriamo che l'agenda delle autorità di vigilanza è sempre up-to-date e ben visibile sul nostro sito e aggiorniamo regolarmente la nostra sezione Notizie importanti informazioni sul nostro lavoro.

Durante il corso dell'anno, abbiamo cambiato il nostro approccio alla raccolta di statistiche sul sito web del GEPD. Per questo motivo, non siamo in grado di segnalare con precisione il numero di visitatori del sito web del GEPD nel 2018. Il nostro nuovo approccio, tuttavia, è stato progettato per garantire che il sito web del GEPD è la protezione dei dati friendly possibile, passando da *decidere di uscire* il monitoraggio a un *opt-in*

processi.

Nell'ambito del sistema di opt-out, i visitatori del sito Internet del GEPD potrebbero seguire le semplici istruzioni fornite nel nostro banner biscotto di scegliere di avere la loro attività sul nostro sito web monitorato. Il nuovo processo di opt-in, tuttavia, farà in modo che siamo solo in grado di tracciare i visitatori del nostro sito web se prevedono esplicitamente noi con il consenso a farlo. Il nuovo sistema sarà lanciato nel mese di gennaio 2019. Fino ad allora, nessun monitoraggio di qualsiasi tipo si svolgerà sul sito web del GEPD.

#### Social media

I social media è diventato indispensabile come strumento di comunicazione. Con la nostra presenza sui tre canali di social media influenti ormai ben consolidata, siamo in grado di utilizzare questi strumenti per raggiungere velocemente e facilmente un pubblico globale.

Mentre Twitter ( @EU\_EDPS ) Resta il nostro strumento di social media più influenti, la nostra presenza sul LinkedIn è in rapida crescita ed è ora anche uno strumento molto influente per le nostre attività di comunicazione. In aggiunta a questo, i nostri sforzi di comunicazione nel corso della Conferenza internazionale di protezione dei dati 2018 e della privacy ha portato ad un aumento significativo del numero di seguaci sul [GEPD YouTube](#)

canale, che cercheremo di costruire su nei prossimi mesi.

La nostra continua crescita sui social media è testimonianza della nostra crescente influenza globale come organizzazione, così come i nostri sforzi per attuare una strategia efficace di social media. Questo ci permette di raggiungere un pubblico sempre più diversificata e globale.



### blog GEPD

Abbiamo lanciato il [blog GEPD](#) di nuovo nel mese di aprile 2016. Da allora, il blog è andato sempre più rafforzandosi. Si tratta di una piattaforma attraverso la quale il GEPD e del garante sono in grado di comunicare su un livello più personale sui loro pensieri, opinioni e attività, così come il lavoro dell'istituzione in generale. Il blog è facilmente reperibile sulla home page del sito web in cui viene sempre visualizzato un breve estratto dal più recente blogpost.

Nel 2018 abbiamo pubblicato 14 blogposts su una serie di argomenti ferenti di f. Tra queste, la Conferenza Internazionale 2018, e-privacy, [gli incontri con GEPD Responsabili della protezione dei dati \(DPO\) e il nuovo regolamento per le istituzioni e gli organi dell'UE](#). Tutte le nostre blogposts sono stati promossi attraverso i nostri canali di social media e molti di loro anche ricevuto l'attenzione dei media.

### 7.1.2 Eventi e pubblicazioni


@EU\_EDPS

**La parola chiave di #GDPRforEU è**

**# responsabilità** . Ciò significa che la protezione dei dati personali deve essere radicata nella cultura delle organizzazioni. Attenersi a

**# protezione dati legge e dimostrare la conformità!**  
**Leggi la nostra scheda [https:// europa.eu/IPY43hU](https://europa.eu/IPY43hU) & Guarda un video**

<https://europa.eu/MM88bY>

#### Il GDPR per EU: la campagna di comunicazione

L'11 dicembre 2018, le nuove regole sulla protezione dei dati per le istituzioni e gli organi dell'Unione europea si applica integralmente. Per completare la nostra attività di sensibilizzazione in corso ( [vedere la sezione 4.1.2](#) ), Abbiamo lanciato una campagna di comunicazione. Anche se dirette principalmente al personale dell'istituzione dell'Unione Europea, abbiamo anche voluto sensibilizzare quelli al di fuori delle istituzioni europee su come le nuove regole loro ei loro diritti possono influire.

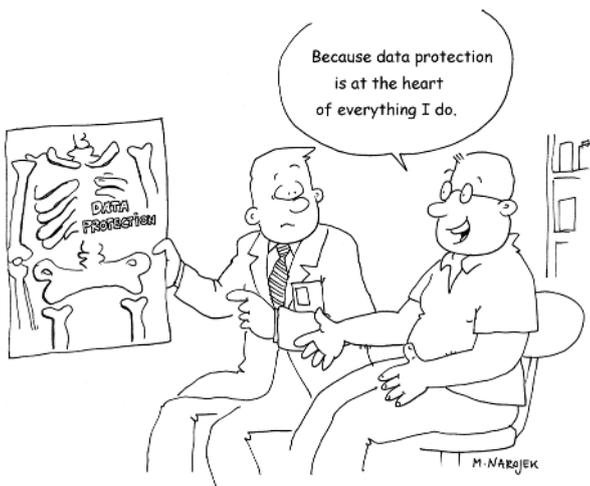
Abbiamo messo insieme un kit di comunicazione per aumentare la consapevolezza circa le nuove regole all'interno delle istituzioni dell'UE e di fornire informazioni pertinenti e utili per tutti i membri del personale dell'UE. Questo kit è stato distribuito a tutti i DPOs istituzione dell'UE in anticipo dell'11 dicembre 2018, per aiutarli a raggiungere i membri dello staff che lavorano nelle loro rispettive istituzioni.

Il kit comprendeva un [il video sulla responsabilità](#) , Un poster per DPO per stampare e distribuire nei loro edifici, opere d'arte per l'uso sul loro canali intranet o di social media e webcam copre da distribuire tra alcuni membri del personale dell'UE. E 'incluso anche tre schede, su [i diritti di protezione dei dati nel quadro delle nuove regole](#) , [le implicazioni delle nuove regole per i dipendenti UE](#) e [garantendo responsabilità](#) . Copie di nuove regole sono state anche preparate e distribuite tra DPO alla riunione GEPD-DPO, che ha avuto luogo a Bruxelles il 12 dicembre 2018 ( [vedere la sezione 4.4.1](#) ).

Per completare la nostra collaborazione con gli RPD, abbiamo lanciato una stampa e social media campagna, volto a sensibilizzare al di fuori delle istituzioni dell'UE. Ciò ha incluso l'utilizzo di Twitter e LinkedIn per fornire

informazioni sulle nuove regole, le loro implicazioni e il ruolo e le attività del GEPD. Oltre ad emettere un [comunicato stampa](#) in data 11 dicembre 2018, abbiamo contattato alcuni media direttamente per cercare di garantire una copertura. Un annuncio è stato pubblicato anche nel politico il 13 dicembre 2018, caratterizzato da un cartone animato coinvolgente.

Gli sforzi sono stati fatti anche per portare il nostro sito e voce di Wikipedia up-to-date, in modo da riflettere la legislazione modificata.



### UE Open Day 2018

In occasione della Giornata dell'Europa, il 5 Maggio 2018 le istituzioni europee hanno aperto le loro porte a tutti i membri del pubblico. L'annuale Giornata aperta UE è un'opportunità per le istituzioni dell'UE per aumentare la trasparenza del loro lavoro e di educare le persone sulle attività dell'UE. Per il GEPD, è la possibilità di aumentare la consapevolezza del pubblico in generale del nostro ruolo e protezione dei dati in generale.

Quest'anno, lo stand GEPD è stato ancora una volta trova nel palazzo Berlaymont della Commissione europea. dipendenti GEPD erano a disposizione dalle ore 10 in poi a rispondere alle domande dei visitatori e incoraggiarli a partecipare al nostro quiz protezione dei dati. software di rilevamento del viso, che tenta di definire una persona di genere, l'età e le emozioni, anche dimostrato popolare e senza dubbio contribuito ad un numero record di persone che partecipano al quiz.

Con la consapevolezza pubblica sulla privacy e la protezione dei dati a un livello più alto, il crescente interesse per la protezione dei dati e il lavoro del GEPD era sia comprensibile e incoraggiante. Non vediamo l'ora di accogliere ancora più persone al nostro stand nel 2019.



@EU\_EDPS

#EUOpenDay 2018 è iniziata. Venite a trovarci!  
La tua privacy conta!

#eudatap #ecberlaymont

### Giornata della protezione dei dati 2018

Il 28 gennaio di ogni anno, le istituzioni dell'UE, le agenzie e gli organismi, nonché gli Stati membri del Consiglio d'Europa, celebrano la Giornata della protezione dei dati. Questo giorno segna l'anniversario del Consiglio d'Europa Convenzione sulla protezione dei dati, nota come Convenzione 108, la legge internazionale di prima vincolanti in materia di diritti delle persone alla protezione dei loro dati personali.

Quest'anno, per l'occasione, i tirocinanti GEPD ha tenuto una conferenza di pranzo il 12 febbraio 2018, incentrato su questioni di protezione dei dati relativi ai modernamento giorno di dating app. Il GEPD e del garante fornito l'apertura e la chiusura osservazioni alla conferenza, che comprendeva i pannelli su temi quali:

- Quali dati personali incontri applicazioni possono elaborare e come usano questi dati;
- i diritti degli individui per richiedere l'accesso ai dati raccolti su di loro;
- etica digitali nel contesto del sito di incontri applicazioni;
- privacy by design;
- algoritmi utilizzati per *incontro* gli utenti di app.

Che si svolgono solo due giorni prima di San Valentino, il tema della conferenza ha avuto successo nella sensibilizzazione sui rischi e dei diritti connessi con le applicazioni ampiamente utilizzate, così come in incoraggiare i giovani a impegnarsi nella protezione dei dati e il dibattito privacy. La conferenza è stata webstreamed in diretta sul nostro sito web, assicurando che era accessibile anche ad un pubblico più ampio.

### notiziario

Dopo il lancio della nostra versione dal nuovo look a metà del 2017, il [GEPD Newsletter](#) è più popolare che mai. Il nuovo formato significa che è ora più accessibile e facile da usare su tutte le piattaforme digitali e pubblicando

più spesso siamo in grado di garantire che i nostri lettori sono tenuti aggiornati sulle nostre ultime attività.

Nel 2018, abbiamo pubblicato nove edizioni del GEPD Newsletter. Tra questi, il nostro speciale edizione di gennaio, in cui abbiamo evidenziato alcune delle nostre attività di alto profilo meno dal 2017, e la nostra edizione Conferenza Internazionale speciale nel mese di settembre. La nostra mailing list continua a crescere, con 3907 persone ora iscritti ai nostri aggiornamenti mensili. Questo serve come un richiamo costante l'importanza e la rilevanza della newsletter come strumento di comunicazione.

### 7.1.3 Relazioni esterne

#### Relazioni con i media

Abbiamo rilasciato dieci **comunicati stampa** e le **dichiarazioni nel 2018**. Questo è paragonabile con i nostri sforzi nel 2017 e dimostra la coerenza del nostro approccio relazioni con i media attuale, che attinge anche sui social media e blog per generare copertura mediatica. Tutti i nostri comunicati stampa sono stati pubblicati sul sito web del GEPD, distribuito alla nostra rete di giornalisti e altri

parti interessate e pubblicata sul sito dell'Unione europea Sala stampa.

Abbiamo anche ricevuto 104 richieste formali da stampa europea e internazionale su una vasta gamma di argomenti.

Alcuni degli argomenti su cui abbiamo ricevuto notevole copertura stampa durante l'anno includono la Conferenza Internazionale 2018, il regolamento sulla protezione dei dati generali (GDPR) e notizie false e lo scandalo di Cambridge Analytica / Facebook. La copertura mediatica è stata particolarmente rilevante in Italia, il paese d'origine del GEPD, Giovanni Buttarelli.

#### visite di studio

Nel 2018, abbiamo ospitato 12 visite di studio presso il GEPD. Come il profilo della protezione dei dati è aumentato, così ha interesse per il nostro lavoro. Anche se vorremmo ospitare ogni gruppo che esprime un interesse per il GEPD e quello che stiamo facendo, con l'alto carico di lavoro che abbiamo dovuto affrontare nel 2018 e lo spazio limitato a disposizione per ospitare queste visite, siamo stati purtroppo costretti ad essere un po' più selettivo.

## GEPD Information & Communication nel 2018:

### le statistiche



#### Media Online:

14 024 Seguaci su Twitter

475 tweets GEPD

9169 Seguaci su LinkedIn

1250 Seguaci su YouTube

#### Eventi e pubblicazioni:

3907 iscritti alla Newsletter

14 | post del blog

#### Relazioni esterne:

10 comunicati stampa

104 richieste formali da stampa

12 visite di studio

516 richieste di informazioni pubbliche

Tuttavia, le visite di studio comprendono una parte importante della nostra strategia di comunicazione, che ci permette di comunicare direttamente con gli studenti, esperti legali, professionisti privacy e altri gruppi influenti per aumentare la consapevolezza circa il lavoro del GEPD e l'Unione europea sulla protezione dei dati e della privacy.

#### Le richieste di informazioni

Il numero di richieste pubbliche di informazioni ricevute dal GEPD è stato l'anno in crescita su anno, e il 2018 non ha fatto eccezione. Infatti, nel 2018 abbiamo assistito ad un enorme aumento delle richieste. Come negli anni passati, la maggior parte di queste richieste in relazione a questioni sulle quali il GEPD ha alcuna competenza.

Uno dei motivi di un aumento significativo esempio delle richieste è stata l'introduzione del GDPR maggio 2018. Abbiamo ricevuto un gran numero di richieste relative all'applicazione di queste nuove regole, anche se non eravamo l'autorità competente a rispondere a loro. La maggiore visibilità del GEPD, sia per effetto del profilo elevato di protezione dei dati e delle nostre attività relative alla Conferenza Internazionale 2018, aiuta anche a spiegare questo aumento.

Rispondiamo a tutte le richieste con informazioni rilevanti per l'inchiesta individuale. Ciò comporta riferendosi individui al servizio rilevante se la loro richiesta non rientra nostra competenza, o fornendo loro le informazioni appropriate per rispondere alle loro ricerca.

#### 7.1.4 L'EDPB

I preparativi per l'EDPB iniziato con largo anticipo del 25 maggio 2018 ( [vedere la sezione 4.1.1](#) ), Quando il Consiglio ha iniziato ufficialmente la sua attività come un organismo dell'UE. Anche se il Consiglio stesso ha un proprio team di comunicazione, il team atti GEPD dell'informazione e della comunicazione in un ruolo di supporto, come e dove richiesto.

In testa fino a maggio 2018, la maggior parte di questo lavoro si è concentrato sul garantire che l'EDPB sarebbe pronto a iniziare a lavorare dal primo giorno. Per farlo, hanno bisogno di un sito web. Abbiamo lavorato a stretto contatto con i colleghi della EDPB per garantire che il loro sito era pronto e perfettamente funzionante in tempo per il lancio del EDPB il 25 maggio

2018, anche assicurando che i membri del personale EDPB hanno ricevuto una formazione su come utilizzare il sito web.

Oltre a questo, abbiamo fornito un sacco di supporto grafico, contribuendo a progettare e produrre pubblicazioni e altro materiale grafico in linea con la corporate identity del EDPB.

Dal lancio del EDPB, abbiamo continuato a sostenere la loro squadra di comunicazione nelle loro attività e partecipare anche in conferenze call regolari organizzati dalla secretar EDPB IAT wi th rappresentanti **ioni Comunicat dall'altro UE autorità per la protezione dei dati (DPA)**, che compongono l'EDPB. Ci auguriamo che questo rapporto produttivo continuerà.

## 7.2 AMMINISTRAZIONE, BILANCIO E PERSONALE

Il ruolo delle risorse umane, bilancio e amministrazione Unità (HRBA) è quello di fornire supporto al Consiglio di Gestione GEPD e le **squadre operative e aiutarli a raggiungere gli obiettivi stabiliti nel [Strategia GEPD 2015-2019](#)** .

L'Unità svolge compiti HR tradizionali, ma è anche responsabile per un'attenta gestione del bilancio institution's e l'implementazione di nuove politiche, che assicurano che la vita lavorativa al GEPD senza intoppi.

2018 è stato un anno molto impegnativo per l'Unità HRBA e il GEPD in generale. Tra le molte altre cose, abbiamo accolto la segreteria europea Consiglio sulla protezione dei dati (EDPB), ha lanciato un concorso di protezione dei dati per aiutare a reclutare nuovi membri del personale, completato i nostri preparativi per il nuovo regolamento sulla protezione dei dati per le istituzioni dell'UE e ha introdotto alcune nuove iniziative HR.

#### 7.2.1 Bilancio e finanze

##### bilancio

Nel 2018, il GEPD è stato assegnato un budget di EUR 14 449 068. Questo ha rappresentato un aumento del 27.59% rispetto al bilancio 2017.

Come nelle precedenti stime, la nostra proposta di bilancio fatta una chiara distinzione tra le cosiddette attività attuali e nuovi. Per le attività in corso, abbiamo continuato con la politica di austerità raccomandato dalla Commissione europea. La maggior parte delle linee di bilancio quindi è rimasta congelata a 0%, con un incremento complessivo del 1,54%. Questo incremento è stato inferiore al costo previsto di vivere al momento del 1,8%, che è stato il massimale proposto dalla Commissione.

Per quanto riguarda le nuove attività, l'aumento del bilancio di 27.59% è venuto principalmente per effetto della costituzione della nuova EDPB. Questo coperto la nostra richiesta per altri sei dipendenti a tempo pieno, così come il budget richiesto per il funzionamento e le attività del Consiglio di Amministrazione, che ha avuto inizio il 25 maggio 2018.

Il tasso di esecuzione del bilancio previsto per il 2018 sarà di circa il 94%. Questo è abbastanza alto date le incertezze connesse con la creazione di un nuovo organo come l'EDPB, e l'impatto sul bilancio questo potrebbe avere.

## Finanza

Per il settimo anno consecutivo, la dichiarazione di affidabilità della t europea Cour dei conti sull'esercizio finanziario 2017 (DAS 2017) non conteneva alcuna osservazione in merito all'affidabilità dei nostri conti annuali.



## procurement

Nel 2018, abbiamo iniziato a lavorare su una nuova iniziativa denominata *Procurement Progetto professionalizzazione*. Noi realizzare il nuovo progetto nel corso del 2019. Ha tre obiettivi principali:

- la nomina di specifici agenti dell'iniziazione operativi in ogni unità operativa e il settore del GEPD, che riceverà una formazione specific sulle procedure di appalto;
- l'attuazione di una soluzione senza, workflow elettronico;
- una revisione delle procedure di appalto esistente con l'obiettivo di migliorare la nostra efficienza e la semplificazione delle procedure attuali.

Nel 2018 abbiamo assegnato tre bandi di gara per un valore di oltre 15.000 euro. Questi erano:

- CAMERON - Media training (60 000,00 EUR)
- Forum Europe - Organizzazione della ICDPPC - Conferenza 2018 (134 900,00 EUR)
- Weber Shandwick - Agenzia di comunicazione (144 000,00 EUR)

Alcuni grandi progetti e contratti sono stati conclusi anche attraverso contratti quadro interistituzionali. Questi erano:

- **DIGIT / DI-07.360-00 (SIDE) / Commissione europea**

1. Il rinnovamento del nostro sistema di gestione dei casi (CMS), VDE / SAAS e servizi di consulenza (Fabasoft)

monitoraggio 2. media online e database di media internazionali (Acqua di disgelo)

- **ITS14 (lotto 2 e 3) / Parlamento europeo**

1. sviluppatori web e Drupal sviluppatori per il GEPD, EDPB e 2018 siti web International Conference

2. Analista IT e sviluppo specialista per l'analisi e lo sviluppo di strumenti informatici

### 7.2.2 Preparazione per la segreteria EDPB

L'EDPB è un organo indipendente, la cui segreteria è fornita dal GEPD. Mentre la segreteria stessa è responsabile di fornire al Consiglio di Amministrazione amministrativa, logistica e supporto analitico, siamo tenuti a garantire che l'EDPB riceve adeguate risorse umane e finanziarie e per fornire supporto amministrativo dove **necessario** ( [vedere la sezione 4.1.1](#) ).

Nel marzo 2018 abbiamo accolto il nuovo segretariato EDPB al primo piano degli uffici del GEPD. Tuttavia, molte altre attività amministrative e logistiche dovevano anche essere completata entro l'EDPB ha iniziato ufficialmente la sua attività come un organo dell'UE sulla 25 maggio 2018.

### decisioni interne

L'EDPB ha iniziato a lavorare lo stesso giorno che il nuovo [Il regolamento generale sulla protezione dei dati \(GDPR\)](#) è diventato pienamente applicabili. E 'stato quindi essenziale per garantire che, a partire dal 25 maggio 2018, tutti i membri staff trasferiti dalle GEPD al EDPB, nonché eventuali nuovi membri del personale EDPB, sarebbe ancora beneficiare degli stessi diritti e sono soggetti alle stesse regole coloro che lavorano per il GEPD.

Abbiamo quindi effettuato una revisione di tutte le decisioni, le linee guida e manuali esistenti e una decisione generale è stato firmato dal direttore GEPD. Mentre alcune decisioni specifiche devono ancora essere aggiornati per tener conto delle particolarità relative alla segreteria EDPB, la maggior parte del lavoro è stato completato.

## Aggiornamento contratti di servizio

Il GEPD ha diversi accordi sui livelli di servizio (SLA) con i fornitori esterni che aiutano i singoli membri del personale e il GEPD, in generale, per svolgere in modo efficace ed efficiente i loro ruoli.

Tutti gli SLA che coprono i membri del personale del GEPD si applicano automaticamente ai membri del personale del segretariato EDPB. Tuttavia, alcuni SLA si riferiscono solo alla fornitura di servizi. Questi avevano bisogno di essere aggiornati per garantire che i membri del personale EDPB potessero fare uso di questi servizi.

Durante la prima metà dell'anno, diversi SLA erano quindi aggiornati per includere l'EDPB. In altri casi, nuove SLA sono stati firmati direttamente tra la segreteria EDPB e il fornitore di servizi. Questo ci ha aiutato a garantire la continuità aziendale e un avvio regolare per la segreteria EDPB.

## Un programma pilota per brevi distacchi

Il 28 UE [autorità per la protezione dei dati \(DPA\)](#) e il GEPD compongono l'EDPB. Una forte cooperazione tra tutti questi membri è essenziale per raggiungere risultati. Per essere veramente efficace, tale cooperazione dovrebbe estendersi oltre esperti di protezione dei dati, gli esperti di risorse umane pure.

Il 29 settembre 2018, abbiamo organizzato un incontro tra le unità HR delle DPA dell'UE per discutere di un programma pilota di EDPB brevi distacchi. Abbiamo voluto discutere le proposte e di scambio, al fine di sviluppare un programma che possa essere di beneficio a tutti DPA.

Il programma fornirà un pool di esperti in diverse aree che vogliono visitare un altro DPA o la segreteria e lo scambio di conoscenze EDPB. Speriamo di lanciare il programma pilota, all'inizio del 2019.

### 7.2.3 Un concorso per gli specialisti della protezione dei dati

Per coprire le esigenze di assunzione sia del GEPD e l'EDPB, abbiamo chiesto al Ufficio europeo di selezione del personale (EPSO) per lanciare un nuovo concorso aperto per 30 amministratori in materia di protezione dei dati.

Sia il GEPD e l'EDPB hanno un crescente bisogno di personale esperto, non solo per coprire il consueto turnover del personale, ma per aiutare entrambe le organizzazioni per adempiere ai loro ruoli e responsabilità in modo efficace. Mentre l'EDPB è un nuovo organo dell'UE in crescita, il GEPD deve assumere nuovo personale per completare le attività aggiuntive a noi ceduti dal legislatore comunitario, come ad esempio la supervisione di Eurojust ([vedere la sezione 4.4.13](#)). V'è quindi evidente la necessità di

un pool di esperti di protezione dei dati altamente qualificati per soddisfare le nostre esigenze future assunzioni.

Questo è il secondo concorso di protezione dei dati organizzati dal GEPD dal 2015. Ci aspettiamo che il nuovo elenco di riserva dei candidati per essere pronti entro la metà del 2019.

### 7.2.4 Il GDPR per EUI: preparazioni HR

Come istituzione dell'UE, il GEPD non è solo responsabile della supervisione e far rispettare le nuove regole sulla protezione dei dati all'interno delle altre istituzioni e organi dell'UE, li deve valere anche per il nostro lavoro e cercare di impostare un esempio per le altre istituzioni a seguire ([vedere le sezioni](#)

[4.1.2 e 8.2](#)).

Il nuovo regolamento riguarda numerose decisioni HR. Abbiamo quindi avviato una revisione completa delle nostre attività di trattamento dei dati HR. Lavorando in stretta collaborazione con la supervisione GEPD e **Unità Enforcement, Protezione dei dati (DPO) e assistente DPO**, abbiamo redatto nuovi record di protezione dei dati e rivisti i nostri avvisi di protezione dei dati al fine di garantire che eravamo pronti per il nuovo regolamento.

### 7.2.5 Migliorare le politiche HR

#### Il kit di benvenuto

Per migliorare l'esperienza di benvenuto per i nuovi membri del personale, la **squadra HRBA mettere insieme un *Welcome Kit***.

Il kit fornisce i nuovi arrivati con informazioni pratiche su come lavorare per il GEPD. Questo include informazioni su chi siamo e cosa facciamo, la gestione del tempo, l'apprendimento e lo sviluppo, il servizio e la sicurezza questioni mediche, tra molte altre cose.

Ci auguriamo che, fornendo nuovi membri del personale con tutte queste informazioni come parte di un kit, li aiuterà a risolvere più rapidamente e facilmente nel mondo del lavoro presso il GEPD.

#### programma di tutoraggio

Il programma di tutoraggio GEPD si rivolge a tutti i nuovi membri del personale. Il suo obiettivo è quello di facilitare l'integrazione dei nuovi arrivati nella nostra istituzione. La natura piuttosto unica del GEPD come istituzione più piccolo dell'Unione europea rende il programma di tutoraggio utile anche per i nuovi membri del personale che ci uniscono da altre istituzioni dell'UE.

Anche se il programma di tutoraggio è in vigore dal momento che il GEPD in sé è stata fondata, abbiamo scoperto che molti membri del personale non erano a conoscenza di ciò che significa essere un mentore comporta. Per affrontare questo problema, abbiamo sviluppato alcune linee guida per i membri del personale del GEPD, che spiega il programma e il ruolo di un mentore in modo più dettagliato.

Un mentore è in grado di fornire il supporto e la guida di un nuovo membro del personale, riducendo lo stress associato con iniziare un nuovo lavoro. E' anche un rapporto che può e deve essere consolidato nel corso dell'impiego del mentee al GEPD. Ci sono vantaggi per entrambe le parti. Il mentee è in grado di girare per il mentore per aiutare a risolvere i problemi, integrando all'interno dell'organizzazione, affermare la propria identità professionale e di apprendimento di nuove competenze. Il mentore beneficia la soddisfazione di aiutare gli altri e la possibilità di visualizzare l'organizzazione da una prospettiva diversa, e potrebbe anche imparare nuovi modi di affrontare le questioni e le attività del mentee.

### anziani attivi

**Il anziano attivo iniziativa cerca di capitalizzare l'esperienza di colleghi in pensione** al fine di garantire che le loro competenze e conoscenze non sono persi. Si tratta di una nuova pratica per il GEPD, lanciato il 29 maggio 2018.

Il processo è volontaria, sia per il membro ritirato personale e l'unità GEPD o settore di attività. Mentre beneficiando del know-how di un ex funzionario può apportare un valore aggiunto al nostro lavoro, riconosciamo anche che non deve sostituire il lavoro di una corrente dipendente GEPD.

Attraverso attingendo alla loro assistenza volontaria, ci proponiamo di mettere l'esperienza di coloro che si sono ora in pensione dal loro lavoro presso le istituzioni europee a buon uso, qualunque sia il loro livello di anzianità quando si ritirarono.

### Assicurandosi che un buon lavoro è sempre riconosciuto

La nostra più recente indagine personale del GEPD ha dimostrato che un buon numero di membri del personale del GEPD si sentono motivati e disposti ad andare il miglio supplementare nel loro lavoro. Tuttavia, c'è sempre spazio per migliorare.

Nel 2018 abbiamo lanciato alcune linee guida volte ad aiutare i manager e gli altri membri del personale di riferimento per dare un migliore riconoscimento per il lavoro svolto dalla sua squadra. Le linee guida spiegano come identificare quali tipi di riconoscimento sono apprezzato da persone diverse e migliori modi di fornire questo riconoscimento.

Non esiste una formula magica che funziona per tutti, quindi è importante che i manager riflettere attentamente su questo argomento, al fine di garantire che le loro squadre ricevono un adeguato riconoscimento per il loro lavoro. Ciò contribuirà ad aumentare la motivazione tra i membri del personale e garantire che esse continuano a fare un ottimo lavoro.

### Il Piano di Continuità Operativa

Il servizio di audit interno (IAS) ha richiesto una profonda revisione e aggiornamento del nostro piano di continuità

(BCP). Abbiamo completato questo processo nel 2018 e il BCP è ora disponibile sulla rete intranet del GEPD.

Revisione del Piano ha coinvolto riformulando un certo numero di articoli della BCP originale. Abbiamo anche bisogno di completare gli allegati del Piano e svolgere un esercizio di test gestione della Business Continuity, che abbiamo fatto il 14 novembre 2018. La relazione sulla esercizio è stato inviato al IAS, in conformità con le loro raccomandazioni.

Per seguire per l'esercizio, la BCP Desk Officer presenterà un piano d'azione, con l'intenzione di avviare un'iniziativa di sensibilizzazione che aiuterà a creare e consolidare una cultura della gestione della continuità operativa tra il personale del GEPD. Sarà anche essere usato per eseguire altri esercizi di test utili.

### Apprendimento e sviluppo

L'attuale GEPD apprendimento e lo sviluppo (L & D) strategia è stata sviluppata nel 2015 e viene messo in pratica ogni anno. 2018 non ha fatto eccezione.

i membri del personale del GEPD sono stati invitati a riflettere sugli esiti dei loro colloqui di valutazione annuali con i loro rispettivi manager di linea e produrre un apprendimento personale e Piano di Sviluppo 2018-2019.

In aggiunta al catalogo di corsi forniti dalla Commissione europea, abbiamo creato alcune sessioni di formazione in-house, tra cui:

- sessioni di pranzo lo strumenti e le procedure utilizzate al GEPD e l'EDPB, finalizzato a nuovi membri del personale;
- Corsi di formazione per preparare il personale per il nuovo regolamento per le istituzioni dell'Unione europea e alla GDPR;
- formazione del team di gestione per la condivisione e l'attuazione di una visione per il futuro, mentre la costruzione squadre impegnate;
- sessioni di formazione del personale per aumentare la consapevolezza dei pregiudizi inconsci, per aiutare a prevenire il burnout e lo stress e su come trovare il giusto equilibrio tra la vita professionale e privata.

Abbiamo anche organizzato una serie di corsi di formazione di comunicazione durante tutto l'anno. Questi avevano lo scopo di sostenere alcuni membri del personale e le autorità di vigilanza in loro preparazione della **2018 Conferenza internazionale di protezione dei dati e della privacy (vedere paragrafo 4.7)**.

## 8. Il ot ti ec Da ta Pr sul fi cio ratt ha GEPD

### 8.1 IL DPO AL GEPD

Con il **Il regolamento generale sulla protezione dei dati (GDPR)** ormai una realtà, ci troviamo di fronte il compito di vivere all'altezza delle grandi aspettative dei cittadini dell'Unione europea e gli altri. Non solo si aspettano che i loro dati personali siano meglio protetti, si aspettano che le autorità di regolamentazione per mantenere le loro promesse e dimostrare di essere all'altezza della sfida di far rispettare queste nuove regole.

Ma anche questo non è sufficiente. Regolatori devono dare l'esempio. Quando trattano dati personali, loro affidati da individui, essi devono garantire che essi sostengono i più alti standard per garantire la protezione delle persone.

La conformità delle istituzioni dell'Unione europea con la legge sulla protezione dei dati era sotto controllo pubblico anche prima che le nuove regole illustrate nel **regolamento 2018/1725**, Applicabile alle loro attività, è entrato in vigore l'11 dicembre 2018 (vedere la sezione 4.1.2). L'UE non può credibilmente chiamare per le organizzazioni e le imprese che operano nell'UE a rispettare le norme comunitarie, se le sue istituzioni non dimostrano che anche loro, sono compatibili. Allo stesso modo, in quanto l'UE di **autorità per la protezione dei dati**, Il GEPD non può aspettarsi di essere attendibile e presa sul serio come un'autorità di vigilanza se non siamo in grado di dimostrare il nostro rispetto.



Con questo in mente, l'ufficio DPO al GEPD, con il sostegno di tutto l'istituto, ha istituito un progetto per gestire il nostro processo di transizione e garantire il rispetto delle nuove norme stabilite ai sensi del regolamento 2018/1725. La protezione dei dati personali non può più essere trattato come un semplice esercizio in conformità. Richiede un

sforzo continuo da tutto l'istituto, orientata a garantire l'uso responsabile delle informazioni personali, se stiamo auditing istituzioni comunitarie, gestione dei reclami, rispondendo alle richieste di informazioni, o svolgere gli ulteriori compiti richiesti di noi dal diritto dell'Unione.

### 8.2 IL PASSAGGIO A UN NUOVO REGOLAMENTO

Il progetto di transizione attuato a GEPD inclusi:

- esaminando le nostre attività di trattamento dei dati e di identificare i rischi che comportano per i diritti e le libertà fondamentali delle persone;
- la preparazione di record di dati personali sulla base dell'articolo 31 del nuovo regolamento, così come i nuovi avvisi di protezione dei dati, che sono necessari per una maggiore trasparenza;
- rivedere il modo in cui gestiamo richieste da individui che desiderano esercitare i loro diritti di protezione dei dati;
- creando una procedura interna per gestire eventuali violazioni dei dati personali elaborati;
- stesura di nuove norme di attuazione DPO e delle necessarie regole interne sulle restrizioni ai diritti dei dati personali sulla base dell'articolo 25 del nuovo regolamento;
- esaminando tutte le attività in cui agiamo controllori come comuni, importanti accordi scritti, le nostre relazioni con i nostri processori e relativi contratti.

L'11 dicembre 2018, quando il nuovo regolamento è entrato in vigore, che avevamo messo in atto tutte le basi necessarie per la conformità. Completeremo i passaggi rimanenti nel progetto di transizione nel 2019.

I nostri sforzi non finirà qui, tuttavia. Abbiamo in programma di istituire un quadro entro il GEPD, sostenuta dai vertici aziendali, che ci permetterà di **fornire ciò che abbiamo definito la protezione in base alla progettazione**. Ciò significa integrare pienamente la protezione dei dati di responsabilità nella cultura della nostra istituzione, che fornisce il massimo livello di protezione per i dati che ci vengono affidati. Questo non è un compito facile, ma crediamo che siamo più che all'altezza della sfida.

### 8.3 CONSULENZA L'ISTITUZIONE E MIGLIORARE IL LIVELLO DI PROTEZIONE

Naturalmente, le nostre attività non si sono solo concentrati sulla preparazione per il futuro. Per tutta la maggior parte dell'anno, le istituzioni dell'UE sono rimasti vincolati dalle regole descritte nel regolamento precedente, [regolamento 45/2001](#).

Come in passato, l'ufficio GEPD DPO ha fornito consulenza su una serie di operazioni di trattamento e delle politiche interne in base alle norme stabilite nel regolamento 45/2001. Abbiamo dedicato particolare attenzione al GEPD siti web, con particolare attenzione l'uso dei cookies per statistiche aggregate, nonché sulla messa a punto del nuovo sito web e app per la [2018 Conferenza internazionale di protezione dei dati e della privacy](#). Abbiamo anche migliorato il modo in cui viene effettuata la raccolta e il trattamento dei dati personali quando l'organizzazione di meeting ed eventi.

### 8.4 RICHIESTE E RECLAMI

Nel 2018, abbiamo ricevuto 11 richieste, di cui nove relativi a richieste di accesso ai propri dati personali di un individuo, elaborato dal GEPD e due richieste interessati per la cancellazione dei dati personali.

Abbiamo anche ricevuto due denunce. Uno riguardava presunto uso illecito di un partecipante caso di contatti condivisi, basati sul consenso, da parte di altri partecipanti. Abbiamo fatto sì che la situazione è stata risolta e i dati cancellati. Un'altra denuncia presunto uso illecito di un subappaltatore di dati personali appartenenti ad una partecipante all'evento. Abbiamo sostenuto il denunciante, in una situazione in cui il subappaltatore aveva usato i dati di propria iniziativa e non su istruzione del GEPD.

Ora stiamo ricevendo un numero crescente di richieste di informazioni e reclami. Questa tendenza è destinata a continuare, ora che gli individui hanno più e più forti diritti di cui le nuove regole sulla protezione dei dati e sono anche più consapevoli di questi diritti.

### 8.5 SENSIBILIZZAZIONE IN SEDE DI GEPD

Il GEPD DPO ha accolto molti nuovi membri del personale e ai tirocinanti nel 2018. Ogni nuovo arrivo presso il GEPD

incontra il DPO per un breve incontro di protezione dei dati personali a induzione, mirato al background formativo e professionale di ogni nuovo membro del personale e il loro ruolo futuro al GEPD. Alcuni degli argomenti trattati sono:

- un'introduzione ai concetti di protezione dei dati di base e la base giuridica applicabile;
- il ruolo dell'RPD presso il GEPD e nelle istituzioni dell'Unione europea;
- preparazione delle nuove norme di protezione dei dati;
- come il DPO può aiutare il personale di esercitare i loro diritti alla protezione dei dati.

riunioni di coordinamento e di informazione del GEPD interni e sezioni DPO sulla intranet GEPD e il sito web sono anche opportunità per raggiungere i membri del personale del GEPD e interlocutori esterni e tenerli aggiornati con le nostre attività.

### 8.6 COLLABORAZIONE CON DPOS nelle altre istituzioni UE

Gli incontri biennali dei DPOs delle istituzioni, degli organi e le agenzie sono una preziosa opportunità per il GEPD DPO per discutere problemi comuni e condividere esperienze e best practice con altri DPO ([vedere la sezione 4.3.1](#)).

Quest'anno, il GEPD ha organizzato la riunione della rete DPO che ha avuto luogo il 30 maggio 2018, in collaborazione con il DPO del Parlamento europeo. L'evento, che ha dimostrato di essere l'ultima riunione prima dell'adozione delle nuove regole, è stato un grande successo. 120 DPO e assistenti DPOs hanno preso parte, contribuendo alla presentazione di casi di studio e dibattiti sui principali problemi incontrati come parte dei loro preparativi per il nuovo regolamento.

Il DPO Ufficio GEPD ha inoltre partecipato alla prima riunione della rete DPO della nuova era, che ha avuto luogo l'11 dicembre 2018, il giorno in cui il nuovo regolamento è entrato in vigore. Tutti DPO hanno lasciato l'incontro con un maggiore senso di responsabilità, consapevole del ruolo che dobbiamo svolgere nel sostenere la protezione dei dati personali, come project manager per la responsabilità nelle istituzioni dell'UE.

## ALLEGATO A - L egalfr amewo rk

Il garante europeo della protezione dei dati è stato istituito dalla **II regolamento (CE) n 45/2001** del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati. Il regolamento è stato basato sull'articolo 286 del trattato CE, ora sostituito dall'articolo **16 della Trattato sul funzionamento dell'Unione europea (TFUE)**. Il regolamento stabilisce altresì norme adeguate per le istituzioni e gli organi in linea con la normativa UE allora vigente in materia di protezione dei dati. È entrato in vigore nel

2001. Una versione del regolamento rivisto, **Regolamento (UE) n 2018/1725**, È entrato in vigore l'11 dicembre 2018.

Dall'entrata in vigore del trattato di Lisbona il 1° dicembre 2009, l'articolo 16 TFUE deve essere considerato come la base giuridica per il GDPR. L'articolo 16 sottolinea l'importanza della protezione dei dati personali in un modo più generale. Sia l'articolo 16 TFUE e l'articolo 8 della **Carta dei diritti fondamentali dell'UE** stabilire che il rispetto delle norme sulla protezione dei dati dovrebbe essere soggetto al controllo di un'autorità indipendente. A livello comunitario, questa autorità è il GDPR.

Altri atti comunitari pertinenti in materia di protezione dei dati sono i seguenti:

- La direttiva 95/46 / CE, che è stato sostituito dal regolamento **2016/679, il II regolamento generale sulla protezione dei dati (GDPR)**, il 25 maggio 2018. La GDPR stabilisce un quadro generale per la legge sulla protezione dei dati negli Stati membri;
- La direttiva 2002/58 / CE relativa alla vita privata e alle comunicazioni elettroniche (Come modificata dalla **direttiva 2009/136**);
- La direttiva sulla protezione dei dati nei settori di polizia e giustizia

Un nuovo regolamento in materia di privacy e comunicazioni elettroniche (ePrivacy) è attualmente in fase di negoziazione ( **vedere la sezione 4.1.3** ).

### sfondo

Articolo 8 del **Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali** prevede un diritto al rispetto per privati

e la vita familiare, soggette a restrizioni consentito solo in 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 per la tutela dei diritti e delle libertà fondamentali che possono essere influenzata dal trattamento di dati personali in una società moderna. La convenzione, nota anche come Convenzione 108, è stata ratificata da più di 40 Stati membri del Consiglio d'Europa, tra cui al I Stati membri dell'UE. Convenzione 108 verrà modificata dal protocollo (STCE n ° 223) al momento della sua entrata in vigore.

La direttiva 95/46 / CE, che è stato il predecessore del GDPR, si è basata sui principi della convenzione 108, ma precisa e sviluppata in molti modi. Il suo obiettivo era quello di fornire un elevato livello di protezione e di una libera circolazione dei dati personali nell'Unione europea. Quando la Commissione ha presentato la proposta di direttiva nei primi anni 1990, ha dichiarato che le istituzioni e gli organi comunitari dovrebbero essere coperti da garanzie giuridiche simili, consentendo loro di prendere parte ad una libera circolazione dei dati personali, nel rispetto della normativa di protezione equivalenti. Tuttavia, fino all'adozione dell'articolo 286 del trattato CE, una base giuridica per un tale accordo è stato carente.

Il 6 aprile 2016, l'UE ha accettato di una grande riforma del suo quadro sulla protezione dei dati, adottando il GDPR per sostituire la vecchia direttiva. Il GDPR è un passo essenziale in avanti nel rafforzamento dei diritti fondamentali dei cittadini nell'era digitale. Si concentra sul rafforzamento dei diritti degli individui, il rafforzamento del mercato interno dell'UE, garantendo più forte applicazione delle norme, snellire i trasferimenti internazionali di dati personali e di definizione di standard globali di protezione dei dati.

In aggiunta a questo, il GDPR aumenta il campo di applicazione territoriale delle norme sulla protezione dei dati dell'UE, introduce sanzioni amministrative, rafforza le condizioni per il consenso e dà alle persone un maggiore controllo sui propri dati personali, in particolare rendendo più facile l'accesso.

Il trattato di Lisbona rafforza la tutela dei diritti fondamentali in modi diversi. Il rispetto della vita privata e familiare e la protezione dei dati personali sono trattati come diritti fondamentali distinti negli articoli 7 e 8 della Carta. Questo è giuridicamente vincolante, sia per le istituzioni e gli organi, e per gli Stati membri dell'UE quando applicano il diritto dell'Unione. La protezione dei dati è anche trattata come soggetto orizzontale di cui all'articolo 16 del TFUE. Questo indica chiaramente che la protezione dei dati è considerata

come ingrediente base di *buon governo*. controllo indipendente è un elemento essenziale di tale protezione.

## Il regolamento (CE) n 45/2001

Dando uno sguardo più da vicino il regolamento 45/2001, si deve rilevare anzitutto che, ai sensi dell'articolo 3 (1), si applica alla *trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nella misura in cui detto trattamento è effettuato nell'esercizio di attività tutto o in parte, che rientrano nell'ambito di applicazione del diritto comunitario*. Tuttavia, dopo l'entrata in vigore del trattato di Lisbona e l'abolizione della struttura a pilastri - a seguito della quale i riferimenti a *istituzioni comunitarie e il diritto comunitario* sono diventati obsoleti - il regolamento in linea di principio copre tutte le istituzioni e gli organi dell'Unione europea, se non nella misura in cui gli altri atti comunitari diversamente specificato.

Le definizioni e la sostanza del regolamento seguono da vicino l'impostazione della direttiva 95/46 / CE. Si potrebbe dire che il regolamento (CE) 45/2001 è l'attuazione della presente direttiva a livello istituzione dell'UE. Ciò significa che il regolamento riguarda i principi generali di trattamento legittimo, di proporzionalità e l'uso compatibile, categorie particolari di dati sensibili, le informazioni da dare alla persona, i diritti della persona, obblighi dei responsabili - l'indirizzamento speciale circostanze a livello UE, se del caso - e con la supervisione, l'esecuzione e rimedi. A capitolo separati con la protezione dei dati personali e della vita privata nell'ambito delle reti di telecomunicazione interne. Questo capitolo è l'implementazione a livello istituzione dell'Unione della precedente direttiva 97/66 / CE relativa alla vita privata e alle comunicazioni.

## Il regolamento (CE) n 2018/1725

Ai sensi dell'articolo 2 (1), il presente regolamento si applica al *trattamento dei dati personali da parte di tutte le istituzioni e gli organi a partire dal 11 dicembre, 2018 dell'Unione*. Tuttavia, esso si applica solo al trattamento dei dati personali da parte di Eurojust dal 12 dicembre 2019 e non si applica al trattamento dei dati personali operative di Europol e l'Ufficio del Procuratore europeo, né al trattamento dei dati personali nell'ambito di attività di cui agli articoli 42 (1), 43 e 44 del TUE, come le attività svolte nell'ambito della politica di sicurezza e di difesa comune. Inoltre, solo l'articolo 3 e il capitolo IX del regolamento si applicano al trattamento dei dati personali operativo entro organi dell'Unione e degli organismi nello svolgimento delle attività di cooperazione giudiziaria in materia penale o la cooperazione di polizia.

Le definizioni e la sostanza del regolamento seguono da vicino l'approccio del GDPR. Si potrebbe dire che il regolamento (CE) n 2018/1725 è l'implementazione del GDPR a livello di istituzione dell'Unione europea. La struttura del regolamento 2018/1725 dovrebbe essere inteso come equivalente della struttura della GDPR e quando le disposizioni seguono il GDPR dovrebbero essere interpretate in modo omogeneo. Ciò significa che il regolamento riguarda i principi generali quali il trattamento corretto e lecito, la proporzionalità e l'uso compatibile, consenso, comprese le condizioni speciali per i bambini, categorie particolari di dati sensibili, così come la trasparenza, l'informazione e l'accesso ai dati personali e dei diritti dei dati soggetto. Esso affronta gli obblighi dei controllori, regolatori comuni e processori, controllo, l'attuazione, rimedi, le passività e le sanzioni. Una sezione specifica si occupa della tutela dei dati personali e della vita privata nell'ambito delle comunicazioni elettroniche. Questa sezione è l'implementazione per le istituzioni e gli organi della direttiva 2002/58 / CE in materia di privacy e comunicazioni elettroniche dell'UE.

Regolamento 45/2001 ha introdotto l'obbligo per le istituzioni e gli organi dell'UE di nominare almeno una persona come **Protezione dei dati (DPO)** e del regolamento 2018/1725 ribadisce questo. Questi agenti hanno il compito di garantire l'applicazione interna delle disposizioni del regolamento, compreso il corretto notifica icazione delle operazioni di trattamento, in modo indipendente. Tutte le istituzioni e maggior parte dei corpi hanno ora un responsabile, e in alcuni casi hanno fatto per molti anni. Questi ufficiali sono spesso in una posizione migliore per fornire consulenza o intervenire in una fase iniziale e per contribuire a sviluppare buone prassi. Poiché l'RPD ha l'obbligo formale di cooperare con il GEPD, questa è una rete molto importante e altamente apprezzata **lavorare con e sviluppare ulteriormente ( vedere la sezione 4.4.1 )**.

## Compiti e competenze del GEPD

I compiti e le competenze del GEPD sono chiaramente descritti nel Capitolo V, in particolare agli articoli 41, 46 e 47 del regolamento 45/2001. Questo è sostituito dal capo VI e gli articoli 52, 57 e 58 del **regolamento 2018/1725 ( vedi allegato B )**, Sia in generale che in termini specifici. L'articolo 41 del regolamento 45/2001 (articolo 52 del regolamento 2018/1725) stabilisce la missione generale del GEPD - per garantire che i diritti fondamentali e le libertà delle persone fisiche, in particolare il loro diritto alla protezione dei dati, rispetto al trattamento dei dati personali da parte delle istituzioni e degli organismi dell'UE. Inoltre, espone per sommi capi alcuni elementi specifici di tale missione. Queste responsabilità generali sono sviluppati e specificati in

Articoli 46 e 47 del regolamento 45/2001 e degli articoli 57 e 58 del regolamento 2018/1725, con un elenco dettagliato di compiti e poteri.

Questa descrizione delle responsabilità, doveri e poteri segue un modello molto simile a quelle delle autorità di controllo nazionali. Questi includono l'udito e l'esame delle denunce, lo svolgimento di altre inchieste, informando controllori e dati soggetti ed effettuare controlli preventivi durante l'elaborazione di operazioni presentano rischi specifici. Il regolamento conferisce al GEPD il potere di ottenere l'accesso alle informazioni e ai locali pertinenti, ove ciò sia necessario per le indagini. Il GEPD può anche imporre sanzioni, che ora comprendono sanzioni amministrative, e adire la Corte di giustizia.

Alcune attività sono di natura speciale. Il compito di consigliare la Commissione e le altre istituzioni dell'UE riguarda le nuove normative - ha sottolineato all'articolo 28 (2) del regolamento 45/2001 e all'articolo 42 del regolamento 2018/1725 con un obbligo formale per la Commissione di consultare il GEPD al momento dell'adozione di una normativa proposta relativa alla protezione dei dati personali - si riferisce anche ai progetti di direttive e altre misure che hanno lo scopo di applicare a livello nazionale o per essere recepite nel diritto nazionale. Si tratta di una funzione strategica che consente al GEPD di guardare implicazioni per la privacy in una fase iniziale e di discutere possibili alternative, anche in settori che facevano parte della *ex terzo pilastro* (di polizia e giudiziaria

cooperazione in materia penale). Monitoraggio sviluppi rilevanti che possono avere un impatto sulla protezione dei dati personali e di intervenire nelle cause dinanzi alla Corte di giustizia sono anche importanti compiti. Inoltre, ai sensi dell'articolo 42 (2), del regolamento 2018/1725, la Commissione europea può consultare il comitato europeo per la protezione dei dati (EDPB), istituito per consigliare la Commissione europea e sviluppare politiche *armonizzate ai sensi della GDPR, su proposte che sono di particolare importanza per la tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali*. In tali casi, l'EDPB e il GEPD *coordinare il loro lavoro al fine di emettere un parere comune*.

L'obbligo di collaborare con le autorità nazionali e gli organi di controllo nella *ex terzo pilastro* è anche di importanza strategica. La collaborazione con gli organi di controllo nella *ex terzo pilastro* consente al GEPD di seguire gli sviluppi in tale contesto e di contribuire a un quadro più coerente per la protezione dei dati personali, a prescindere dal

*pilastro* o dal contesto specifico. Sotto il quadro giuridico precedente, non c'era alcun modello coerente unico per controllo coordinato. L'articolo 62 del regolamento 2018/1725 consente ora per la realizzazione di un unico modello per il controllo coordinato del **sistemi di informazione su larga scala** e di organi dell'Unione, uffici o agenzie da parte del GEPD e delle autorità di vigilanza nazionali.

## ALLEGATO B - Estratto dalla Regolazione (UE) 2018/1725

### Articolo 41 - Informazione e consultazione

1. Le istituzioni e gli organismi dell'Unione informano il garante europeo al momento di elaborare provvedimenti amministrativi e le regole interne relative al trattamento dei dati personali da parte di un'istituzione o organismo dell'Unione, da solo o insieme ad altri.
2. Le istituzioni e gli organi dell'Unione si consultano sulla protezione dei dati europea in sede di elaborazione delle norme interne di cui all'articolo 25.

### Articolo 42 - consultazione legislativa

1. La Commissione, in seguito all'adozione di proposte per un atto legislativo, di raccomandazioni o di proposte al Consiglio ai sensi dell'articolo 218 del TFUE o nella preparazione di atti delegati o atti di esecuzione, consultare il garante europeo della protezione dei dati in cui v'è un impatto sulla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.
2. Qualora un atto di cui al paragrafo 1 è del particolare senza imporre per la tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali, la Commissione può inoltre consultare il comitato di protezione dei dati europea. In tali casi il Garante europeo della protezione dei dati e il Comitato europeo per la protezione dei dati devono coordinare il loro lavoro al fine di emettere un parere comune.
3. Il consiglio di cui ai paragrafi 1 e 2 deve essere fornito per iscritto entro un periodo massimo di otto settimane dal ricevimento della richiesta di consultazione di cui ai paragrafi 1 e 2. In caso di urgenza, o nei casi appropriati, la Commissione può ridurre la scadenza.
4. Il presente articolo non si applica quando la Commissione è tenuta, ai sensi del regolamento (UE) 2016/679, di consultare il Consiglio europeo della protezione dei dati.

### Articolo 52 - Garante europeo della protezione dei dati

1. La protezione dei dati europea è istituita.
2. Per quanto riguarda il trattamento dei dati personali, della protezione dei dati europea ha il compito di assicurare che i diritti e le libertà fondamentali delle persone fisiche, e in particolare il diritto alla protezione dei dati, sono rispettati da parte delle istituzioni e degli organi dell'Unione.
3. La protezione dei dati europea è competente per il controllo e garantire l'applicazione delle disposizioni del presente regolamento e di ogni altro atto dell'Unione in materia di tutela dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali da un'istituzione dell'Unione o del corpo, e di fornire alle istituzioni e degli organi dell'Unione e soggetti di dati su tutte le questioni relative al trattamento dei dati personali. A tal fine, la protezione dei dati europea assolve i compiti di cui all'articolo 57 ed esercita i poteri attribuitigli dall'articolo 58.
4. Il regolamento (CE) n 1049/2001 si applica ai documenti in possesso del garante europeo della protezione dei dati. La protezione dei dati europea adotta le modalità di applicazione del regolamento (CE) n 1049/2001 per quanto riguarda tali documenti.

### Articolo 57 - Compiti

1. Fatte salve le altre compiti stabiliti dal presente regolamento, la protezione dei dati europea:
  - a) monitorare e far rispettare l'applicazione del presente regolamento da parte delle istituzioni e degli organi dell'Unione, con l'eccezione del trattamento dei dati personali da parte della Corte di giustizia nell'esercizio delle sue funzioni giurisdizionali;

- b) promuovere la consapevolezza e la comprensione dei rischi, regole, tutele e diritti in relazione al trattamento. Attività rivolte specificamente per i bambini ricevono una particolare attenzione;
  - c) promuovere la consapevolezza dei controllori e processori dei loro obblighi derivanti dal presente regolamento;
  - d) su richiesta, fornire informazioni a qualsiasi soggetto di dati concernenti l'esercizio dei loro diritti ai sensi del presente regolamento e, se del caso, cooperare con le autorità di vigilanza nazionali a tal fine;
  - e) gestire denunce presentate da un soggetto di dati, o da un ente, organizzazione o associazione a norma dell'articolo 67, e indagare, nella misura appropriata, l'oggetto della denuncia e di informare il denunciante dello svolgimento e l'esito della indagine entro un termine ragionevole, in particolare se sono necessari ulteriori indagini o di coordinamento con un'altra autorità di vigilanza;
  - f) condurre indagini in merito all'applicazione del presente regolamento, anche sulla base delle informazioni ricevute da un'altra autorità di vigilanza o di altro ente pubblico;
  - g) fornisce consulenza, su propria iniziativa o su richiesta, tutte le istituzioni e gli organi dell'Unione sulle misure legislative e amministrative relative alla tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali;
  - h) vigilare sugli sviluppi rilevanti, in quanto hanno un impatto sulla protezione dei dati personali, in particolare lo sviluppo delle tecnologie dell'informazione e della comunicazione;
  - i) adottare clausole contrattuali tipo di cui all'articolo 29 (8) e al punto (c) dell'articolo 48 (2);
  - j) stabilire e mantenere un elenco in relazione alla necessità di proteggere i dati di valutazione di impatto a norma dell'articolo 39 (4);
  - k) partecipare alle attività del Consiglio europeo per la protezione dei dati;
  - l) alle funzioni di segreteria del comitato europeo per la protezione dei dati, ai sensi dell'articolo 75 del regolamento (UE) 2016/679;
  - m) dare consigli sul trattamento di cui all'articolo 40 (2);
  - n) autorizzare clausole contrattuali e le disposizioni di cui all'articolo 48 (3);
  - o) tenere registri interni di violazioni del presente regolamento e delle misure adottate a norma dell'articolo 58 (2);
  - p) esegue ogni altro compito connessi alla protezione dei dati personali; e
  - q) adotta il proprio regolamento interno.
2. La protezione dei dati europea deve facilitare la presentazione di denunce di cui alla lettera (e) del paragrafo 1 da un modulo di presentazione denuncia che può anche essere completato elettronicamente, senza escludere altri mezzi di comunicazione.
  3. L'esecuzione dei compiti della protezione dei dati europea è gratuito per la persona interessata.
  4. Quando le richieste sono manifestamente infondata o eccessiva, in particolare a causa del loro carattere ripetitivo, della protezione dei dati europea possono rifiutarsi di dar seguito alla richiesta. La protezione dei dati europea sostiene l'onere di dimostrare il carattere manifestamente infondata o eccessiva della richiesta.

## Articolo 58 - Poteri

1. La protezione dei dati europea avrà i seguenti poteri di indagine:
  - a) per ordinare il controller e il processore di fornire tutte le informazioni necessarie per l'espletamento dei suoi compiti;
  - b) a svolgere indagini in forma di audit protezione dei dati;
  - c) a notificare al controllore o il processore di una presunta violazione del presente regolamento;
  - d) per ottenere, dal controller e il processore, l'accesso a tutti i dati personali ea tutte le informazioni necessarie per lo svolgimento dei suoi compiti;
  - e) per ottenere l'accesso a tutti i locali del controllore e il processore, compreso di qualsiasi apparecchiatura di elaborazione dati e mezzi, conformemente al diritto dell'Unione.

2. La protezione dei dati europea avrà i seguenti poteri correttivi:

- a) di emettere avvertimenti ad un controllore o processore che intendono operazioni di trattamento sono suscettibili di violare disposizioni del presente regolamento;
- b) emettere richiami ad un controllore o un processore in cui le operazioni di lavorazione hanno violato disposizioni del presente regolamento;
- c) di adire il controller o il processore in questione e, se necessario, al Parlamento europeo, il Consiglio e la Commissione;
- d) per ordinare il controllore o al processore di soddisfare le richieste della persona interessata per esercitare i suoi diritti ai sensi del presente regolamento;
- e) ordinare il controllore o processore per portare operazioni di trattamento in conformità con le disposizioni del presente regolamento, se del caso, in un modo specificato ed entro un periodo determinato;
- f) per ordinare il controllore di comunicare una violazione dei dati personali della persona;
- g) imporre una limitazione temporanea o definitiva compreso il divieto di trasformazione;
- h) ordinare la rettifica o la cancellazione dei dati personali o limitazione del trattamento conformemente agli articoli 18, 19 e 20 e la notificazione di misure ai destinatari ai quali i dati personali sono stati comunicati ai sensi dell'articolo 19 (2) e l'articolo 21;
- i) di imporre una sanzione amministrativa ai sensi dell'articolo 66, nel caso di mancato rispetto da parte di un'istituzione dell'Unione o del corpo con una delle misure di cui ai punti (d) a (h) e (j) del presente paragrafo, a seconda le circostanze di ciascun caso;

- j) di ordinare la sospensione dei flussi di dati a un destinatario in uno Stato membro, un paese terzo o ad un'organizzazione internazionale.

3. La protezione dei dati europea avrà i seguenti poteri autorizzativi e di consulenza:

- a) di consigliare gli interessati nell'esercizio dei loro diritti;
- b) consigliare la controllore secondo la procedura di consultazione preliminare di cui all'articolo 40, e ai sensi dell'articolo 41 (2);
- c) di emettere, su propria iniziativa o su richiesta, pareri alle istituzioni e agli organi dell'Unione e al pubblico su qualsiasi argomento relativo alla protezione dei dati personali;
- d) di adottare clausole di protezione dei dati standard di cui all'articolo 29 (8) e al punto (c) dell'articolo 48 (2);
- e) di autorizzare clausole contrattuali di cui alla lettera (a) dell'articolo 48 (3);
- f) di autorizzare intese amministrative di cui alla lettera (b) dell'articolo 48 (3);
- g) di autorizzare operazioni di trattamento norma atti adottati ai sensi dell'articolo 40 di attuazione (4).

4. La protezione dei dati europea ha il potere di adire la Corte di giustizia alle condizioni previste dai trattati e di intervenire nelle cause dinanzi alla Corte di giustizia.

5. L'esercizio dei poteri conferiti al garante europeo della protezione dei dati ai sensi del presente titolo Ar è soggetto ad adeguate garanzie, tra cui ricorsi giurisdizionali efficaci e giusto processo, di cui al diritto dell'Unione.

## Allegato C - Lista di Autorità Protettive di Officiers O

Consiglio dell'Unione europea (CONSILIUM)	<i>Reyes OTERO ZAPATA</i>
Parlamento europeo (PE)	<i>Secondo SABBIONI</i>
Commissione Europea (CE)	<i>Martin KRÖGER</i>
Corte di giustizia dell'Unione europea (CURIA)	<i>Sabine Hackspiel</i>
Corte dei conti (ECA)	<i>Johan Van Damme</i>
Comitato economico e sociale europeo (CESE)	<i>Constantin CHIRA-PASCANUT</i>
Comitato delle regioni (CdR)	<i>Michele ANTONINI</i>
Banca Europea degli Investimenti (BEI)	<i>Pelopida Donos</i>
Servizio europeo per l'azione esterna (SEAE)	<i>Emese SAVOIA-KELETI</i>
Mediatore europeo (EO)	<i>Juliano FRANCO</i>
Europeo della protezione dei dati (GEPD)	<i>Massimo ATTORESI</i>
Comitato europeo per la protezione dei dati (EDPB)	<i>João Silva</i>
Banca centrale europea (BCE)	<i>Barbara EGGL</i>
Europeo per la lotta antifrode (OLAF)	<i>Veselina TZANKOVA</i>
Centro di traduzione degli organismi dell'Unione europea (CdT)	<i>Martin GARNIER</i>
Ufficio europeo di Unione proprietà intellettuale (EUIPO)	<i>Mariya Koleva</i>
Agenzia per i diritti fondamentali (FRA)	<i>Nikolaos FIKATAS</i>
Agenzia per la cooperazione fra i regolatori nazionali dell'energia (ACER)	<i>Marina ZUBAC</i>
Agenzia europea per i medicinali (EMA)	<i>Stefano MARINO</i>
Ufficio comunitario delle varietà vegetali (UCVV)	<i>Mariya Koleva</i>
Fondazione europea per la formazione professionale (ETF)	<i>tiziana Ciccarone</i>
Asilo europeo di sostegno per ufficio (UESA)	<i>Alexandru George Grigore</i>
Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)	<i>Athena BOURKA</i>
Fondazione europea per il miglioramento delle condizioni di vita e di lavoro (Eurofound)	<i>Maria-Angeliki STAMATOPOULOU</i>
Osservatorio europeo delle droghe e delle tossicodipendenze (OEDT)	<i>Ignacio Vázquez MOLINI</i>
European Food Safety Authority (EFSA)	<i>Claus REUNIS</i>
Agenzia europea per la sicurezza marittima (EMSA)	<i>Radostina NEDEVA</i>
Centro europeo per lo sviluppo della formazione professionale (CEDEFOP)	<i>Robert STOWELL</i>
Istruzione, gli audiovisivi e la cultura (EACEA)	<i>Panagiota Kalyva</i>
Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA)	<i>Michaela SEIFERT</i>
Agenzia europea di controllo della pesca (EFCA)	<i>Marta Ramila HIDALGO</i>
Europea Centro satellitare dell'Unione europea (CSUE)	<i>Esther MOLINERO</i>
Istituto europeo per l'uguaglianza di genere (EIGE)	<i>Ramunas LUNSKUS</i>
Agenzia del GNSS europeo (GSA)	<i>Ezio VILLA</i>

Agenzia ferroviaria europea (ERA)	Zografia PYLORIDOU
I consumatori, la salute e l'alimentazione Agenzia esecutiva (CHAFEA)	Tobias Kohlhof
Centro europeo per la prevenzione e il controllo delle malattie (ECDC)	Andrea IBER
Agenzia europea dell'ambiente (EEA)	Olivier CORNU
Fondo europeo per gli investimenti (FEI)	Paolo SINIBALDI
Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne (FRONTEX)	Nayra PEREZ
Europea degli strumenti finanziari e dei mercati (ESMA)	Sophie VUARLOT-DIGNAC
Agenzia europea per la sicurezza aerea (EASA)	Stephan MICK
Agenzia esecutiva per le piccole e medie imprese (EASME)	Elke RIVIERE
Agenzia esecutiva Innovazione e Reti (INEA)	Caroline maion
Autorità bancaria europea (EBA)	Joseph MIFSUD
Agenzia europea delle sostanze chimiche (ECHA)	Bo BALDUYCK
Agenzia europeo della ricerca Executive Council (ERCEA)	Cristina Ganguzza
Agenzia esecutiva per la ricerca (REA)	Evangelos TSAVALOPOULOS
Comitato europeo per il rischio sistemico (ESRB)	Barbara EGGL
Fusion for Energy (ITER)	Signora Angela Bardenhewer-RATING
SESAR Joint Undertaking (SESAR)	Laura GOMEZ GUTIERREZ
Componenti e sistemi elettronici per la leadership europea (ECSEL)	Anne SALAÛN
Dell'impresa comune Clean Sky (COMUNE CLEAN SKY)	Bruno Mastantuono
Impresa comune sui medicinali innovativi (IMI JU)	Sebastien PECHBERTY
Celle a combustibile e idrogeno impresa comune (FCH)	Georgiana BUZNOSU
Europea delle assicurazioni e delle pensioni Occupazioni (EIOPA)	Catherine COUCKE
Accademia europea di polizia (CEPOL)	Ioanna PLIOTA
Istituto europeo di innovazione e tecnologia (EIT)	Nora TOSICS
Agenzia europea per la difesa (EDA)	Clarisse RIBEIRO
Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC)	Geoffrey DEVIN
Istituto europeo per gli studi sulla sicurezza dell'Unione (IUESS)	Nikolaos CHATZIMICHALAKIS
Agenzia europea per la gestione operativa su larga scala sistemi IT in spazio di libertà, sicurezza e giustizia (eu-LISA)	Fernando Luis POCAS DA SILVA
Impresa comune Shift2Rail (S2R JU)	Isaac GONZALEZ GARCIA
Consiglio Risoluzione singolo (SRB)	Esther Brisbois
Europol (EUROPOL)	Daniel Drewer
Bioindustrie impresa comune (BBI JU)	Marta CAMPOS ITURRALDE

## ALLEGATO D - L istofpriorcheckandnon - priorcheckopinions

### Amministrazione

#### Per la lotta antifrode, denuncia e della finanza

- Indagini amministrative e procedimenti disciplinari, (EBA), 25 lug 2018 (2017-1083)
- indagini amministrative, (BEI), 18 lug 2018 (2017-1071)
- Svolgimento delle indagini da parte del servizio di sicurezza del segretariato generale del Consiglio (SGC), (CONSIGLIO), 25 Apr 2018 [UPDATE] (2017-0216)
- Whistleblowing, (EMSA) 3 aprile 2018 (2017-0303)
- Whistleblowing, (OEDT), 22 marzo 2018 (2016-1083)
- Whistleblowing, (FRA), 21 marzo 2018 (2.016-0.737)
- Denunce e rilevanti di frode interna problemi, (REA), 21 marzo 2018 (2014-0178)
- Whistleblowing, (GEPD), 15 marzo 2018 (2017-0493)
- Whistleblowing, (ECHA), 15 marzo 2018 (2015-1029)
- Amministrative inquiries and disciplinary proceedings, (EIT) 17 gennaio 2018 (2016-1165)
- soluzioni ragionevoli, (CONSIGLIO), 18 settembre 2018 (2018-0592)
- Disciplinari e Grievance Investigations, (EFTA), 18 settembre 2018 (2017-1142)
- Selezione di Confidential Consiglieri, (FEI) 18 settembre 2018 (2017-1043)
- procedura informale per i casi di molestie, (FEI), 18 settembre 2018 (2017-1042)
- Nulla osta di sicurezza, (ESA) 18 settembre 2018 (2017-1004)
- attività professionale dopo aver lasciato il servizio, (EO), 19 LUGLIO 2018 (2017-1064)
- gestione sottoperformance, (CE) 19 luglio 2018 (2.017-0.395)
- Personale Riclassificazione, (EACEA), 10 lug 2018 (2017-1062)
- I dati sulla salute, (GSA), 10 luglio 2018 (2018-0589)
- CSISLA - richiesta di rimborso per le spese mediche, (SEAE), 3 luglio 2018 (2017-0986)
- Performance Management, (EFTA), 20 giu 2018 (2017-1094)
- dati sanitari, (EIOPA), 24 mag 2018 (2.017-0.284)
- L'accesso e l'utilizzo del sistema di posta elettronica del Mediatore, (EO), 12 aprile 2018 (2017-1059)
- Molestie, (EIOPA), 10 aprile 2018 (2017-0916)
- Rimpatrio di personale espatriato UE per motivi di salute, (SEAE), 4 aprile 2018 (2016-0778)
- Incontri Organizzazione, (ECDC), 20 mar 2018 (2017-1078) - Non controllo preliminare
- OHC Gravidanza Self-Assessment dati, (BEI), 12 marzo 2018 (2016-0614)
- Le indagini di sicurezza, (SEAE), 7 dicembre 2018 (2017-1107)
- ILOAT e Corte EFTA reclami nel campo delle risorse umane, (EFTA), 23 nov 2018 (2017-1141)
- verifiche di sicurezza sui dipendenti di contraenti esterni che devono accedere alle EUIs, (SEAE), 30 ottobre 2018 (2016-0894)
- Sicurezza Verificazione delle risorse esterne, (EUIPO), 15 OTTOBRE 2018 (2.017-0.350)
- Accreditamento e Notifica di diplomatici di delegazioni dell'Unione al Paese Ospite, (SEAE), il 5 ottobre 2018 (2017-1099)

- Gestione di tutti i diritti lasciare l'elaborazione delle richieste ricevute per il rimborso delle annuali visite mediche pre-assunzione ricevuto medica esami / distanze, (SRB), 8 marzo 2018 (2017-0853)
  - procedura di mobilità, (CONSIGLIO) 21 febbraio 2018 (2018-0031)
  - Aiuti sociali e finanziarie l'assistenza sociale e la consulenza sul rimborso delle spese mediche per la sede e le delegazioni dell'UE, (SEAE), 21 FEBBRAIO 2018 (2016-0779)
  - I dati amministrativi e finanziari relativi ai diritti individuali dei membri del personale, (SRB), 9 febbraio 2018 (2017-0852) - non controllo preventivo
  - Tempo modulo di gestione di Sysper, (SRB) 7 febbraio 2018 (2017-0850) - Non controllo preliminare
  - Pronto soccorso registri di intervento, (CONSIGLIO) 26 gennaio 2018 (2017-0969)
  - L'accesso ai locali dell'ECDC, (ECDC), 17 gennaio 2018 (2017-1077) - Non controllo preliminare
- Valutazione (360 ° e valutazione del personale)**
- Rapporti periodo di prova, (GSA), 9 Ottobre 2018 (2017-1066)
  - Ioni Promot e riclassificati Ioni f ICAT, (CDT), 26 settembre 2018 (2016-0292)
  - Staff valutazione, (CDT), 26 Settembre 2018 [UPDATE] (2016-0011)
  - Promozione, (CSUE), 6 settembre 2018 (2014-0603)
  - Valutazione del personale, (EACEA), 10 luglio 2018 (2017-1061)
  - Multi-source Feedback per i manager, (CONSIGLIO), 18 Apr 2018 (2018-0170)
  - Statistiche sulla produzione individuale e tempestività, (EUIPO) 8 marzo 2018 (2017-0841)
- Borse di studio e appalti pubblici**
- Grants aggiudicazione e la gestione nel contesto di Orizzonte 2020 programma quadro, (REA), 10 dicembre 2018 (2017-1080)
  - Gestione e concessione di sovvenzioni Orizzonte 2020, (SESAR JU), 10 dicembre 2018 (2017-1076)
  - Borse di studio, (IET), il 10 dicembre 2018 (2017-1070)
  - Grants Management, (CHAFFEA), 10 dicembre 2018 (2017-1068)
  - H2020 Grants aggiudicazione e la gestione (INEA), il 10 dicembre 2018 (2017-1037)
  - Concedere gestione in portale partecipante, (EASME), 10 dicembre 2018 (2.017-0.977)
  - Selezione Registrazione e gestione di esperti indipendenti nell'ambito del 7 ° PQ e Orizzonte 2020 (H2020) programmi quadro, (REA), 25 settembre 2018 (2017-1085)
  - gestione esperto indipendente Orizzonte 2020, (SESAR JU), 25 settembre 2018 (2017-1075)
  - Experts H2020, (BBI), 25 settembre 2018 (2017-1073)
  - Gestione di esperti, (EACEA), 25 settembre 2018 (2017-1063)
  - Esperto Indipendente di gestione, (CHAFFEA), il 25 settembre 2018 (2017-1053)
  - Selezione e gestione di esperti indipendenti per la realizzazione di parti di H2020, (INEA), 25 settembre 2018 (2017-1038)
  - gestione esperti in Partecipante portal, (EASME), 25 settembre 2018 (2017-0976)
  - gestione esperti all'esterno portale partecipante, (EASME) 31 luglio 2018 (2017-1040)
  - Concede gestione esterna portale partecipante, (EASME) 31 luglio 2018 (2017-1039)
  - gestione esperti fuori programma COSME portale partecipante, (EASME) 31 luglio 2018 (2017-1036)
  - Concedere gestione esterna portale partecipante al programma COSME, (EASME) 31 Luglio 2018 (2017-1035)
  - Contratto di rinnovo di processo, (EBA), 19 lug 2018 (2017-1082)
  - il rinnovo contrattuale, (EIOPA), 31 maggio 2018 (2017-0769)
  - Procedure di appalto, (EASME), 22 marzo 2018 (2017-1058)

- Indipendente esperti di gestione, (FCH 2JU), 30 gennaio 2018 (2.018-0.030)
- concessione di una sovvenzione e di gestione, (FCH 2JU), 30 gennaio 2018 (2018-0029)

#### Reclutamento

- Selezionare tment ioni recrui e administrat gestione ive di agenti locali (LA) nelle delegazioni UE, (SEAE), il 30 novembre 2018 (2017-1106)
- Selezionare ioni Reclutamento e Administrat ive di gestione per il personale internazionale per le missioni PSDC dal civile di pianificazione SEAE e condotta (CPCC), (SEAE), il 6 novembre 2018 (2017-1105)
- Procedura di selezione per l'ECDC, (CE), il 16 ottobre 2018 (2018-0039)
- Reclutamento, (BEI), 6 settembre 2018 [UPDATE] (2015-1052)
- Reclutamento, (BEI), 6 settembre 2018 (2017-1072)
- Reclutamento, (EFTA), 20 giu 2018 (2017-1093)
- RECLUTAMENTO temporanei, (EMSA), 6 giugno 2018 (2015-0439)
- Selezionare ioni tment Recrui e Administrat ive di gestione per i professionisti Junior presso le delegazioni dell'UE (JPDs), (SEAE), 13 marzo 2018 (2016-0772)
- Assunzione di personale: Tas END e tirocinanti, (SRB), 2 Marzo 2018 (2017-0851)
- Nuove antipasti e abbandoni, (EFTA), 22 Febbraio 2018 (2017-1143) - non controllo preventivo
- Selezione e gestione amministrativa di Blue tirocinanti libri in sede centrale del SEAE e presso le delegazioni dell'UE, (SEAE) 12 febbraio 2018 (2.016-0.771)

- Selezione e reclutamento di TA CA tirocinanti END e interrelazioni IMS, (S2R JU), 8 febbraio, 2018 (2018-0119)
- Procedura di assunzione direttore esecutivo, (CEPOL) 29 gennaio 2018 (2017-0787)

#### Attività principale

- analisi di sicurezza automatizzata dei servizi internet crittografate con SSL utilizzati dalla rete SEAE, (SEAE), 7 dicembre 2018 (2015-0593) - Non controllo preliminare
- nuova notifica 'sistema AAC' della DG SANTE, (CE) 29 ottobre 2018 (2.017-0.803)
- Domanda per il ritorno (FAR), (FRONTEX), 26 settembre 2018 (2017-0874)
- Aggiornamento del corrente mutua assistenza Broker (MAB), (CE), 24 settembre 2018 (2018-0698)
- Sottrazione internazionale di minori mediatore di attività, (EP), 12 settembre 2018 (2016-0731)
- social media monitoring, (BCE), 21 marzo 2018 (2017-1052)
- Erasmus + online Regime di sostegno linguistico, (EACEA), 1 marzo, 2018 (2014-1154) - Non controllo preliminare
- Erasmus + online Regime di sostegno linguistico, (EACEA), 1 marzo, 2018 (2014-1154) - Non controllo preliminare
- Pannello Stakeholder Quality Assurance (SQAP), (EUIPO), 20 febbraio 2018 (2017-0845)
- misure dell'UE autonome restrittive, (Consiglio), 5 Febbraio 2018, [aggiornamento per 2.012-0.725], (2018-0106)

## ALLEGATO E - List of Opinions and formal Comments on legislative proposals

### opinioni

Si prega di fare riferimento alla [sito web del GEPD](#) per traduzioni e sommari esecutivi.

Nel 2018 il GEPD ha formulato pareri sui seguenti argomenti (data di pubblicazione tra parentesi):

- Pacchetto della Commissione sulle elezioni europee libere ed eque ( [18 dicembre 2018](#) )
- Aggiornamento del sistema di informazione visti ( [13 dicembre 2018](#) )
- Un New Deal per i consumatori ( [5 OTTOBRE 2018](#) )
- Sicurezza di carte d'identità e documenti di soggiorno dei cittadini dell'Unione e dei loro familiari ( [10 agosto 2018](#) )
- Gli strumenti digitali e processi in materia di diritto societario ( [26 Luglio 2018](#) )
- Settore pubblico (PSI) La direttiva riutilizzo ( [10 July 18](#) )
- Privacy by Design ( [31 Maggio 2018](#) )
- L'interoperabilità tra i sistemi di informazione su larga scala UE ( [16 Aprile 2018](#) )
- manipolazione online e dei dati personali ( [19 mar 2018](#) )
- Scambio di dati tra Europol e paesi terzi ( [14 marzo 2018](#) )
- Proposta di regolamento del Consiglio sulle decisioni di giurisdizione in materia matrimoniale e in materia di responsabilità genitoriale e sulla sottrazione internazionale di minori (Bruxelles II rifusione) ( [15 febbraio 2018](#) )

### formali Commenti

Si prega di fare riferimento alla [sito web del GEPD](#) per le traduzioni francesi e tedesche.

Nel 2018 il GEPD ha formulato osservazioni formali sui seguenti argomenti (data di pubblicazione tra parentesi):

- Border europeo e Coast Guard ( [3 dicembre 2018](#) )
- covered bond e le obbligazioni garantite controllo pubblico ( [12 Ottobre 2018](#) )
- Facilitare l'uso delle informazioni finanziarie e di altri per la prevenzione, individuazione, indagine e perseguimento di certi penali dei recinti ( [10 Settembre 2018](#) )
- Assicurazione della responsabilità civile derivante dalla circolazione dei veicoli a motore ( [26 Luglio 2018](#) )
- Revisione del regolamento OLAF ( [24 Luglio 2018](#) )
- Migrazione e protezione internazionale ( [18 LUGLIO 2018](#) )
- controlli sulla pesca ( [18 LUGLIO 2018](#) )
- Copyright nel mercato unico digitale ( [3 Luglio 2018](#) )
- Free-flusso di dati non personali nell'Unione europea ( [8 giugno 2018](#) )
- Autorità del lavoro europea (ELA) ( [30 maggio 2018](#) )
- Proiezione di investimenti diretti esteri verso l'Unione europea ( [12 aprile 2018](#) )
- frode dell'IVA e la cooperazione amministrativa ( [8 marzo 2018](#) )
- Sistema d'informazione visti (VIS) per includere i dati sui visti lunga durata e documenti di soggiorno ( [9 febbraio 2018](#) )

# ALLEGATO F - Spiechesbythe Supervisorand Assistant Supervisorin 2018

## Parlamento europeo

Assistente supervisore, *La protezione dei dati e gli aspetti sulla privacy dei l'attuale generazione di registratore di dati di evento e il monitoraggio sonnolenza avanzata*, discorso durante l'udienza del *Requisiti di omologazione per i veicoli a motore per quanto riguarda la loro sicurezza generale e la salvaguardia dei veicoli Occupanti e vulnerabili utenti della strada*, Parlamento Europeo, Bruxelles (29 novembre 2018).

Garante aggiunto, discorso al LIBE udienza del e-prove, Parlamento Europeo, Bruxelles (27 novembre 2018).

Garante aggiunto, discorso alla terza riunione del Gruppo d'esame parlamentare congiunta sulla Europol, Parlamento Europeo, Bruxelles (25 Settembre 2018).

Supervisore, discorso all'udienza LIBE sul caso Facebook / Cambridge Analytica, Parlamento Europeo, Bruxelles (25 Giugno 2018).

Assistente supervisore, *La protezione dei dati in Intelligenza Artificiale e di alta Performing Computing*, discorso ai dati seminario Driven Innovation & AI dati Conferenza, Parlamento Europeo, Bruxelles (6 giugno 2018).

Garante aggiunto, discorso a interruzioni: opzioni per il futuro accordo di condivisione dei dati UK-EU, Parlamento Europeo, Bruxelles (5 Giugno 2018).

Supervisore, discorso al Congresso Mondiale Quinto libertà di ricerca scientifica, Parlamento Europeo, Bruxelles (12 Aprile 2018).

Supervisore, discorso al LIBE sulla relazione annuale 2017, Parlamento Europeo, Bruxelles (20 marzo 2017).

Supervisore, *la supervisione del GEPD di Europol: attività 2017 e lavori in corso*, discorso alla riunione del Gruppo d'esame parlamentare congiunta sulla Europol, Parlamento Europeo, Bruxelles (19 marzo 2018).

Garante aggiunto, discorso in occasione della seconda riunione del Gruppo d'esame parlamentare congiunta sulla Europol, Sofia, Bulgaria (19 marzo 2018).

Garante aggiunto, discorso *Sessione informativa sulla riforma del regolamento sulla protezione dei dati*, Giornata di protezione dei dati, Parlamento europeo, Lussemburgo (31 gennaio 2018).

## Consiglio

Garante, incontro DAPIX sull'interoperabilità, Bruxelles (18 Aprile 2018).

Assistente supervisore, *Quantum of informazioni personali memorizzate nel PNR scende a info-bacini nazionali*, discorso alla conferenza *L'attuazione pratica della direttiva Passenger Name Record*, Sofia, Bulgaria (21 febbraio 2018).

Assistente supervisore, *GDPR sotto il profilo politico e di vista normativo*, discorso alla conferenza generale del regolamento sulla protezione dei dati, Sofia, Bulgaria (29 gennaio 2018).

## Commissione europea

Assistente supervisore, *elezioni libere ed eque e di un dibattito democratico informato e pluralista. Passi concreti per garantire che il mondo online supporta un dibattito democratico informato e pluralista*, intervento al Colloquio annuale sui diritti fondamentali 2018 "La democrazia in Europa, Bruxelles (26-27 novembre 2018).

Assistente supervisore, *Digitalizzazione del settore energetico - sfide e vantaggi per i consumatori. Problemi di privacy e soluzioni*, discorso durante La Settimana Europea dell'Energia Sostenibile - EUSEW 2018 - Conferenza, Bruxelles (5-6 giugno 2018).

## Altre istituzioni e gli organi dell'UE

Assistente supervisore, *Allontanandosi dalla libertà sintonia v. La sicurezza*, discorso alla Accademia di diritto europeo (ERA) conferenza sulla libertà e la sicurezza, L'Aia, Paesi Bassi (22-23 novembre).

Assistente supervisore, *Prospettive future di ingegneria privacy*, discorso durante l'annuale Privacy Forum 2018, Barcellona, Spagna (13-14 giugno 2018).

Garante, il video discorso alla Università AGH, Cracovia, Polonia (6 giugno 2018).

Assistente supervisore, *Radar il servizio di guardia: Hai controllato il radar del vostro reparto di comunicazione al fine di evitare collisioni con il nuovo regolamento?* discorso alla riunione GEPD-DPO, Bruxelles (31 Maggio 2018).

## conferenze internazionali

Assistente supervisore, *Facilitare trasferimento dati*, contributo al seminario *Regolamentazione dei dati personali in un'economia dell'innovazione: Prospettive UK-francesi*, Parigi, Francia (6 Dicembre 2018).

Assistente supervisore, *Global Development di Legge sulla Privacy e Brexit: La differenza tra accordo e non-deal*, interventi a protezione dei dati World Forum, Privacy, fiducia, rischio, sicurezza, Londra, Regno Unito (20-21 novembre 2018).

Supervisor, il contributo video alla protezione dei dati in Africa Summit, Mauritius (19-23 novembre 2018).

Assistente supervisore, *Diritto alla Privacy in Digital Era*, discorso alla conferenza *Fiorente in una società data-enabled*, Buckinghamshire, Regno Unito, (1 novembre 2018).

Supervisor, discorso di chiusura *Discutere Etica: Dignità e rispetto in una vita guidata dai dati*, 40 ° Conferenza Internazionale di Data Protect ions e Pr ivacy Commissari, Parlamento Europeo, Bruxelles (25 ottobre 2018).

Garante, si muovono più lentamente e sistemare le cose. Relazione della Creative Room, discorso alla 40 ° Conferenza internazionale di protezione dei dati e della privacy, Bruxelles (21-25 Ottobre 2018).

Assistente supervisore, *Caratteristiche di base di protezione dei dati nel contesto umanitario*, intervento al workshop *2 ° Serie di lavoro delle linee guida sulla protezione dei dati per le azioni umanitarie*, evento collaterale alla 40 ° Conferenza internazionale di protezione dei dati e della privacy, Bruxelles (21-25 ottobre 2018).

Garante, intervento al convegno seminario 108+: la Convenzione sulla protezione dei dati globali, evento collaterale alla 40 ° Conferenza Internazionale di Data Protect ions e commissari ivacy Pr, Bruxelles (21-25 ottobre 2018).

Garante, intervento al seminario Il futuro per l'azione collettiva sotto la GDPR (Art. 80),

evento collaterale alla 40 ° Conferenza internazionale di protezione dei dati e della privacy, Bruxelles (21- 25 Ottobre 2018).

Assistente supervisore, *Artificiale Intel Ligence in azioni umanitarie*, intervento al workshop *Dal Privacy per Etica: uso improprio, mancato uso, e il bene pubblico*, evento collaterale alla 40 ° Conferenza internazionale di protezione dei dati e della privacy, Bruxelles (21-25 ottobre 2018).

Supervisor, *Scegli umanità: Mettere dignità di nuovo in digitale*, l'apertura di discorso alla 40 ° Conferenza Internazionale di Data Protect ions e Pr ivacy Commissari, Bruxelles (24 Ottobre 2018).

Assistente supervisore, *La nuova tecnologia, la raccolta dei dati e della privacy - dove possiamo trovare l'equilibrio?* discorso alla 6 ° Conferenza annuale QED nt. "Cybersecurity, Bruxelles (17 ottobre 2018).

Assistente supervisore, *prossima ondata di ICT - connettività il bilanciamento e la privacy*, discorso alla FT-ETNO Summit 2018 pt. Review, Reboot, Revive: un'agenda futuro per l'Europa, Bruxelles (15 Ottobre 2018).

Assistente supervisore, *Sorveglianza per la sicurezza pubblica scopi. Quattro pilastri di interferenza accettabile nel diritto fondamentale alla privacy*, discorso alla conferenza *Diritto alla privacy nell'era digitale*, Varsavia, Polonia (20- 22 settembre 2018).

Assistente supervisore, *Generale Regolamento protezione dei dati (GDPR) come chiave per una migliore controllo del trattamento dei dati personali*, discorso al seminario *Aplicació del Reglament europeu de Protecció Tornei, primer Passos*, Barcellona Spagna (14 giugno 2018).

Assistente supervisore, *Privacy by Design in Teoria e nel mondo reale*, intervento al 7 ° privacy su Internet Network Engineering (IPEN) workshop organizzato dal GEPD e l'Univerciat Politècnica de Catalunya, Barcellona, Spagna (13 Giu 2018).

Assistente supervisore, *La nozione di 'dati personali' in settori di pubblica utilità*, il contributo video alla GDPR convegno: un cambiamento positivo per l'utilità aziende? Sofia, Bulgaria (13 giugno 2018).

Assistente supervisore, *Sfruttando reti transnazionali* discorso alla conferenza Agora Forum: *Steady As She Goes? Mondo complesso di L'UE Navigazione Oggi*, Bruxelles (7-8 giugno 2018).

Assistente supervisore, *Molti percorsi di riforma della legge sulla protezione dei dati in Europa* discorso alla conferenza

*Protezione dei dati personali in Polonia e Belgio*,  
Bruxelles (5 giugno 2018).

Supervisore, Commissione austriaca dei Giuristi, Vienna, Austria (31 maggio 2018).

Supervisor, il contributo di video all'8 europeo della protezione dei dati di giorni (EDPD), Berlino, Germania (14 Maggio 2018).

Garante aggiunto, discorso alla *stato globale di protezione dei dati tavola rotonda* a RightsCon 2018, Toronto, Canada (16-18 maggio 2018).

Supervisore, 4 ° Congresso Internazionale 2018 ASSO DPO, Milano, Italia (8 maggio 2018).

Assistente supervisore, *La protezione dei dati personali nel quadro delle forze di polizia e istituzioni giudiziarie*, discorso alla Conferenza di primavera, Tirana, Albania (3-04 MAGGIO 2018).

Assistente supervisore, *Social media, micro-targeting e campagna politica: sfide e opportunità per le autorità di protezione dei dati*, discorso alla Conferenza di primavera, Tirana, Albania (3-4 maggio 2018).

Assistente supervisore, *Automated individuale decisionali e Profiling sotto la GDPR - Come il GDPR affronta i concetti?* discorso alla conferenza annuale sul diritto europeo della protezione dei dati 2018 Focus sul regolamento sulla protezione dei dati generali, Bruxelles (19-20 aprile 2018).

Assistente supervisore, *Importanza della GDPR*, discorso *GDPR e Marketing*, GSMA Mobile World Congress, GSMA programma ministeriale, Barcellona, Spagna (26 -28 Febbraio 2018).

Supervisor, il contributo video da Il marocchino conferenza internazionale sulla privacy e la protezione dei dati in Africa-CNDP, Casablanca, Marocco (22 febbraio 2018).

Supervisor, il contributo video alla dati Forum del Commonwealth 2018, Gibilterra (21-23 febbraio 2018).

Supervisore, Osservazioni conclusive di Giovanni Buttarelli formulato il 11 ° Computers International, la privacy e la protezione dei dati Conferenza, Bruxelles (25 gennaio 2018).

Assistente supervisore, *Regolamentare per i risultati*, discorso al computer, Privacy e protezione dei dati (CPDP) 2018, *Internet degli Enti*, Bruxelles (24-26 gennaio 2018).

## altri eventi

Supervisor, il contributo video da Il Regolamento Europeo sulla privacy (GDPR): ALCUNE Riflessioni Sugli Impatti, Roma, Italia (20 Dicembre 2018).

Supervisor, il contributo video al Giornata della Trasparenza, Prevenzione della corruzione, Trasparenza e privacy: Quale bilanciamento ?, Venezia, Italia (20 dicembre 2018).

Supervisor, il contributo video al Concorso avanzata Seminario, Istituto Universitario Europeo (EUI), Firenze, Italia (15 dicembre 2018).

Supervisor, il contributo video conferenza annuale per i diritti umani, Tallin, Estonia (10 dicembre 2018).

Supervisor, il contributo video al 2018-2019: Protezione dei dati: un biennio Rivoluzionario, Roma-Camera dei Deputati, Roma, Italia (11 dic 2018).

Supervisor, il contributo video conferenza su Intelligenza Artificiale, Varsavia, Polonia (30 novembre 2018).

Garante, Sześć miesięcy stosowania RODO. Europejska perspektywa na pierwsze doświadczenia, intervento al convegno Konwentu Ochrony danych i Informacji 2018, Lodz, Polonia (23 novembre 2018).

Supervisore, Convegno Nazionale Siamo tutti spiati? per la 17a edizione del premio P.Piazzano di giornalismo scientifico, Novara, Italia (17 Novembre 2018).

Garante aggiunto, le minacce moderne (terrorismo e sicurezza informatica) e l'accesso ai dati elettronici: la protezione dei dati e altre limitazioni nel campo della giustizia e della sicurezza, discorso al Consiglio di Sicurezza il commercio di Confederazione europea dei sindacati indipendenti, Bruxelles (15 novembre 2018 ).

Supervisor, il contributo video al AGI Presidenza: Invito ad intervenire al Convegno Nazionale AGI, Bologna, Italia (27 ottobre 2018).

Supervisor, il contributo video in vita dopo la GDPR: regole di buona protezione dei dati e le prospettive per il futuro, Szeged, Ungheria (22-26 ottobre 2018).

Supervisor, il contributo di video a Cosa Sarà, la Trasformazione digitale e La nostra vita quotidiana Pavia, Italia (19-21 ottobre 2018).

Supervisor, il contributo di video per decodificare Symposium 2018, oltre il capitalismo di sorveglianza: alla ricerca della sovranità digitale d'Europa, Barcellona, Spagna (16-17 ottobre 2018).

Garante, Accountability Strumenti per Ente pubblico. Esperienze di istituzioni, agenzie e organismi, discorso alla Responsabilità Workop sotto la GDPR - come implementare, dimostrare e incentivare esso, Parigi, Francia (5 ottobre 2018).

Supervisor, il contributo video al CHAM2018, Costruire il sistema sanitario Europeo, Parigi, Francia (28-29 settembre 2018).

Supervisor, il contributo video da Friends of Europe - seminario Giovani Leader europei, Valletta, Malta (13- 15 settembre 2018).

Supervisor, il contributo video al Industrial Revolution 4.0: Economia digitale, la protezione dei dati e conformità Best-Practice, la Lettonia (7-8 settembre 2018).

Supervisor, il contributo video da UnionCamere - La disciplina Europea in materia di tutela della privacy Ed il Registro delle Imprese, Roma, Italia (9 luglio 2018).

Supervisore, la vita dopo la GDPR: le norme sulla protezione dei dati buone e le prospettive per il futuro, Bruxelles (27 giugno 2018).

Supervisore, discorso alla Ambasciatori Cocktail riceventi per l'ICDPPC 2018, Bruxelles (5 giugno 2018).

Garante, Problemy Społeczne i zawodowe Informatyki, discorso presso l'Università di Varsavia, Varsavia, Polonia (29 maggio 2018).

Garante, Zakres terytorialny obowiązywania RODO un najbliżsi Sasiedzi Unii Europejskiej, discorso alla conferenza 10 ° Sicurezza in Internet pt. Ochrona danych Osobowych, Varsavia, Polonia (25 Maggio 2018).

Garante, Ogólne rozporządzenie o ochronie danych Jako część reformy bezpieczeństwa danych w Europie. Czym jest w Świecie RODO NIS / eIDAS / privacy / AML / PSD2 / eEvidence / eFracht ecc, intervento al convegno scientifico Wyzwania prawne związane z początkiem stosowania Ogólnego rozporządzenia o Ochronie danych (RODO), Danzica, Polonia (28 Aprile 2018).

Supervisore, Privacy, protezione dei dati e della sicurezza informatica nell'era della IA, Bruxelles (24 aprile 2018).

Garante, l'impatto del regolamento sulla protezione dei dati generali sulle istituzioni finanziarie, discorso

al 9 ° FinanzplatzFrühstück (Financial Center colazione), Francoforte, Germania (17 Aprile, 2018).

Garante aggiunto, discorso introduttivo alla conferenza ad alto livello tavola rotonda di lavoro su fiscalità e delle Entrate Collection nell'era della protezione dei dati: come le agenzie possono fare Sfida un'opportunità, Bruxelles (16 Aprile 2018).

Garante, garanzie essenziali di protezione dei dati nel settore delle forze dell'ordine in epoca di sistemi interoperativo, su larga scala IT, conferenza durante la celebrazione del 15 ° anniversario della European Digital Rights (Edri), Bruxelles (12 aprile 2018).

Garante, Czy Nowy Lad prawny zadziała w praktyce? Rola organów danych ochrony, Sadow i STAU w wykładni prawa ochrony danych Osobowych, intervento al convegno 4. Forum Prawa Mediów Elektronicznych, GDPR, Wroclaw, Polonia (aprile 10-11

2018).

Garante, Dokumentacja przetwarzania danych Osobowych w instytucjach Unii Europejskiej, intervento alla conferenza tecnologica Nowe Zasady zabezpieczania danych Osobowych, czyli RODO w praktyce, Varsavia, Polonia (28 marzo 2018).

Supervisor, discorso al Diritto ed economia delle Piattaforme digitali, Roma Tre, Roma, Italia (22 marzo 2018).

Supervisor, il contributo video da Auditel conferenza presso la Camera dei Deputati italiana, Roma, Italia (15 Febbraio 2018).

Supervisor, il contributo video al Le regole Sono Cambiate: privacy UE 679/16, Pordenone, Italia (23 febbraio 2018).

Supervisor, il contributo video da Auditel conferenza presso la Camera dei Deputati italiana, Roma, Italia (15 Febbraio 2018).

Garante, Création du CEPD et les linee guida Dernières, intervento al 14e Conférence annuelle Nouveau protezione dei dati reglement, Parigi, Francia (8 febbraio 2018).

Supervisor, il contributo video alla Westminster eForum Keynote Seminario: La protezione dei dati e il quadro normativo in via di sviluppo, Bruxelles (25 gennaio 2018).

Supervisor, il contributo video La rivoluzione Europea della Privacy, il regolamento UE 679/2016, Padova, Italia (22 Gennaio 2018).

## ALLEGATO G - C OMP osition of GEPD SECRETARIATO



### Direttore e gabinetto

Leonardo CERVERA NAVAS  
*Direttore*

Christian D'CUNHA  
*Capo di Gabinetto del GEPD*

Ernani Cerasaro  
*Politica di Assistente amministrativo*

Anna colaps  
*Politica Assistant*

Sylvie PICARD  
*Coordinatore del controllo interno*

Maria José SALAS MORENO  
*Assistente amministrativo*

Martine VERMAUT  
*Assistente amministrativo*

### Supervisione e l'esecuzione

Delphine HAROU  
*Ad capo ad interim di unità*

Petra CANDELIER  
*Responsabile del Reclami e Contenzioso*

Bénédicte RAEVENS  
*Capo di EUROPOL Supervisione*

Ute Kallenberger  
*Capo di ispezioni*

Owe LANGFELDT  
*Capo di consultazioni*

Stephen Andrews  
*Vigilanza e applicazione Assistant*

Guillaume BYK  
*Ufficio legale*

Evanthia CHATZILIASI  
*Ufficio legale*

Graça COSTA  
*Ufficio legale*

Fanny COUDERT  
*Ufficio legale*

Elena FIERRO  
*Ufficio legale*

Barbara GIOVANELLI  
*Etica Policy Officer digitale*

Dirk HOMANN  
*Ufficio legale*

Xanthi KAPSOSIDERI  
*Ufficio legale*

Anna Larsson Stattin  
*Consigliere giuridico / esperto nazionale distaccato*

Francoise MAYEUR  
*Vigilanza e applicazione Assistant*

Anne NOEL  
*Vigilanza e applicazione Assistant*

Maria Veronica PEREZ ASINARI  
*Ufficio legale*

Aikaterini POULIOU  
*Ufficio legale*

Snezana Srdic  
*Ufficio legale*

Tereza STRUNCOVA  
*Ufficio legale*

Zsofia SZILVASSY  
*Ufficio legale*

## Politica e consultazione

Anna Buchta  
*Ad capo ad interim di unità*

Olivier MATERIA  
*Responsabile della Cooperazione internazionale*

Zsuzsanna BELENYESSY \*  
*Ufficio legale*

Sandra BETTI  
*Politica e consultazione Assistant*

Veronique CIMINA  
*Ufficio legale*

Priscilla DE LOCHT  
*Ufficio legale*

Claire GAYREL  
*Ufficio legale*

Mario GUGLIELMETTI  
*Ufficio legale*

Amanda JOYCE  
*Politica e consultazione Assistant*

Laurent LIM  
*Ufficio legale*

Sophie LOUVEAUX  
*Ufficio legale*

Claire-Agnes MARNIER  
*Ufficio legale*

Lara SMIT  
*Ufficio legale*

Matthias Wildpanner-GUGATSCHKA  
*Consigliere giuridico / esperto nazionale distaccato*

Agnieszka ZAPOROWICZ  
*Ufficio legale*

## Politica IT

Achim Klabunde  
*Capo settore*

Massimo ATTORESI  
*Tecnologia e sicurezza dei dati  
protezione dei*

Andy Goldstein  
*Tecnologia e Security Officer LISO*

Dina KAMPOURAKI  
*Tecnologia e Security Officer*

Malgorzata LAKSANDER \*  
*Tecnologia e Security Officer*

Xabier Lareo  
*Tecnologia e Security Officer*

Frederik LINDHOLM  
*Assistente amministrativo*

Robert RIEMANN  
*Tecnologia e Security Officer*

## Records Management

Luisa PALLA  
*Capo settore*

Marta CÓRDOBA HERNÁNDEZ  
*Assistente amministrativo*

Kim Thien Le  
*Assistente amministrativo*

Séverine NUYTEN  
*Assistente amministrativo*

Constantin Stancu  
*Archivista*

Maria TIGANITAKI  
*Assistente amministrativo*

## Informazione e comunicazione

Olivier ROSSIGNOL  
*Capo settore*

Francesco Albinati  
*Informazione e Communication Officer*

Isabelle BARON  
*Informazione e Communication Officer*

Thomas HUBERT  
*Assistente Graphic Designer*

Courtenay MITCHELL  
*Informazione e Communication Officer*

Veronica MORO  
*Informazione e Communication Officer*

Parminder MUDHAR  
*Informazione e Communication Officer*

Agnieszka Nyka  
*Informazione e Communication Officer*

Benoît PIRONET  
*Sviluppatore web*

Filippo SEGATO  
*Informazione e Communication Officer*

## Risorse umane, bilancio e l'amministrazione

Marian SANCHEZ LOPEZ  
*Ad capo ad interim di unità*

Cláudia BEATO  
*HR Assistant*

Pascale Beeckmans  
*HR Assistant*  
GEMI

Laetitia BOUAZZA-ALVAREZ  
*HR Assistant GECO LSO*  
*Tirocini Coordinatore*

Angelo Fassari  
*Assistente amministrativo*

Sebastian GALEA  
*assistente finanziario*

Laurent HAMERS  
*assistente finanziario*

Sophie Jeannon  
*Assistente amministrativo*

Julia MOLERO MALDONADO  
*assistente finanziario*

Marco Moreschini  
*Ufficiale HR / esperto nazionale distaccato LSO*

Carolina POZO-LOPEZ \*  
*assistente finanziario*

Karina REMPEZ  
*HR Ufficiale L & D*  
*Coordinatore*

Anne-Françoise REYNDERS  
*HR Ufficiale*

Jean-Michel VERSTAEN

*assistente finanziario*

Christophe Walravens

*Acquisti e Responsabile Finanza*

Caroline WOUSSEN-DUBUISSEZ \*

*assistente finanziario*

## EDPB Segreteria

Isabelle Vereecken

*Capo della segreteria EDPB*

Katinka BOJNAR

*Consigliere giuridico / esperto nazionale distaccato*

Hannelore DEKEYSER

*Ufficio legale*

greet Gysen

*Informazione e Comunicazione Responsabile*

Sarah HANSELAER

*Informazione e Comunicazione Responsabile*

Ahmed IMMOUN

*Tecnologia e Security Officer*

Joelle Jouret

*Ufficio legale*

Zoi KARDASIADOU

*Consigliere giuridico / esperto nazionale distaccato*

Peter Kraus

*Tecnologia e Security Officer*

Fabienne MOLLET

*Assistente amministrativo*

Hanna OBERSTELLER

*Consigliere giuridico / esperto nazionale distaccato*

Effrosyni Panagou

*Assistente della Segreteria EDPB*

Andrei Petrovici

*Tecnologia e sicurezza Assistant*

Romain ROBERT

*Ufficio legale*

Luis Segura

*Archivista*

João Silva

*Legal Officer DPO*

Jasminka TOKALIC

*Assistente amministrativo*

Anne-Marie VANDENBERGHEN

*Assistente amministrativo*

Anna Zawila-NIEDZWIECKA

*Consigliere giuridico / esperto nazionale distaccato*

\*i membri dello staff che hanno lasciato il GEPD nel corso del 2018







## Entrare in contatto con l'UE

### Di persona

In tutta l'Unione europea ci sono centinaia di centri d'informazione Europe Direct. È possibile trovare l'indirizzo del centro più vicino a voi: <https://europa.eu/europa-direct>

### Al telefono o tramite e-mail

Europe Direct è un servizio che risponde alle vostre domande sull'Unione europea. Potete contattare questo servizio:

- numero verde 00 800 6 7 8 9 10 11 (taluni operatori potrebbero fatturare queste chiamate),
- al seguente numero di serie: +32 22999696 o
- per e-mail tramite: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

## Ricerca di informazioni sull'UE

### in linea

Informazioni sull'Unione europea in tutte le lingue ufficiali dell'UE è disponibile sul sito web Europa all'indirizzo:

[https://europa.eu/european-union/index\\_en](https://europa.eu/european-union/index_en)

### pubblicazioni dell'UE

È possibile scaricare o ordinare liberi e prezzo pubblicazioni dell'UE a: <https://publications.europa.eu/en/publications>. Più copie di pubblicazioni gratuite possono essere ottenute contattando Europe Direct o il vostro centro di informazione locale (vedi [https:// europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en) ).

### diritto dell'UE e documenti correlati

Per l'accesso alle informazioni giuridiche dell'UE, compresa tutta la normativa UE a partire dal 1952 in tutte le versioni linguistiche ufficiali, andare a EUR-Lex all'indirizzo: <http://eur-lex.europa.eu>

### dati aperti dalla UE

Il portale Open Data UE ( <http://data.europa.eu/euodp/en> ) Fornisce l'accesso al set di dati da parte dell'UE. I dati possono essere scaricati e riutilizzati per libero, sia a fini commerciali e non commerciali.

