“PRIVACY E PUBBLICA AMMINISTRAZIONE, LA NUOVA SFIDA”

E-PRIVACY 2017 AUTUMN EDITION

Venezia, 13 e 14 ottobre 2017
Tribunale di Rialto a Venezia

Avv. Valentina Longo

Iniziativa del Garante

Iniziativa del Garante

74 lettere a:

Ministri

Presidenti di autorità indipendenti

Presidenti CSM, Corte dei conti, Avvocatura dello Stato, enti centrali e agenzie

Presidenti regioni, Conferenza Stato regione, Conferenza Stato città, Upi e Anci

Iniziativa del Garante

Documenti orientativi:

“Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali”

Linee guida sui responsabili della protezione dei dati (RDP) – Gruppo di lavoro art.29

13 dic 2016, emendate il 5 aprile 2017

Priorità di intervento

*“L’avvicinamento al Regolamento. Individuare le priorità e gestire il cambiamento” **

1. designazione del Responsabile della protezione dei dati – RDP (artt.37-39)

2. istituzione del Registro delle attività di trattamento (art. 30 e C171)

3. notifica delle violazioni dei dati personali (c.d. *data breach*, art.33 e 34)

* Francesco Modafferi, Dirigente Libertà Pubbliche e Sanità

Priorità di intervento - RDP

Responsabile della protezione dei dati RDP o *DPO – Data Protection Officer* – artt. 37-38 (C97)

fulcro del processo di responsabilizzazione

Designazione (art.37) **obbligatoria** per trattamenti effettuati da un'**autorità pubblica** o da un **organismo pubblico***

può essere nominato **un unico RDP** per più autorità pubbliche, secondo struttura organizzativa e dimensione

qualità professionali, conoscenza norme, prassi, capacità di assolvere i compiti

* con eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali

Priorità di intervento - RDP

Linee guida sui responsabili della protezione dei dati

"**autorità pubblica**" - "**organismo pubblico**"

definizione conforme all'ordinamento nazionale, autorità nazionali, regionali e locali, oltre una serie di organismi di diritto pubblico

svolgimento di funzioni pubbliche e esercizio di pubblici poteri **svolte da persone fisiche o giuridiche di diritto pubblico o privato**, trattamento simile a quello autorità pubblica **il WP29 raccomanda la nomina**

Ente pubblico o organismo di diritto pubblico

art. 2, paragrafi 1 e 2, della direttiva 2003/98/CE del Parlamento europeo e del Consiglio

Ai fini della presente direttiva si intende per:

1) "ente pubblico", le autorità statali, regionali o locali, gli organismi di diritto pubblico e le associazioni formate da una o più di tali autorità oppure da uno o più di tali organismi di diritto pubblico

Ente pubblico o organismo di diritto pubblico

2) "organismo di diritto pubblico", qualsiasi organismo:

a) istituito per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale

b) dotato di personalità giuridica

c) la cui attività è finanziata in modo maggioritario dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico, oppure la cui gestione è soggetta al controllo di questi ultimi, oppure il cui organo d'amministrazione, di direzione o di vigilanza è costituito da membri più della metà dei quali è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico

Direttiva 2014/24/UE

Priorità di intervento - RDP

Designazione (art.37)

RDP può essere dipendente del titolare o del responsabile oppure assolvere i suoi compiti in base a un contratto di servizi

Il titolare del trattamento o il responsabile del trattamento pubblica i **dati di contatto RDP** e li comunica all'autorità di controllo

Priorità di intervento - RDP

Criteri di scelta RDP

newsletter n. 432 del 15 settembre 2017

- verificare la presenza di **competenze ed esperienze specifiche**
- **non sono richieste attestazioni** (non equivalgono ad abilitazioni) formali sul possesso delle conoscenze o l'iscrizione ad appositi albi professionali
- RDP deve **conoscere** anche **norme e procedure amministrative** che caratterizzano lo **specifico settore** di riferimento

Priorità di intervento - RDP

- privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere
- la normativa attuale non prevede un albo dei RDP

enti e imprese valuteranno autonomamente il possesso dei requisiti necessari per svolgere i compiti da assegnare

Priorità di intervento - RDP

Posizione (art.38)

- **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali
- **risorse necessarie** per assolvere ai compiti e per mantenere la propria conoscenza specialistica (**autonomia**)
- non riceve alcuna istruzione per quanto riguarda l'esecuzione di tali compiti (**indipendenza**)
- non è rimosso e penalizzato per l'adempimento dei compiti

Priorità di intervento - RDP

- riferisce direttamente al vertice (posizione)
- gli interessati possono contattare RDP per tutte le questioni relative al trattamento e per l'esercizio dei diritti
- è tenuto al **segreto** o alla **riservatezza** in merito all'adempimento dei suoi compiti
- può svolgere altri compiti, purché non in conflitto di interessi

Priorità di intervento - RDP

Compiti (art.39)

- **informare e fornire consulenza** al titolare, al responsabile del trattamento, ai dipendenti Su obblighi del regolamento o altre disposizioni UE o SM relative alla protezione dei dati

- **sorveglia sull'osservanza del regolamento**, di altre disposizioni UE o SM nonché delle **politiche del titolare del trattamento o del responsabile** del trattamento compresi l'attribuzione delle responsabilità, la **sensibilizzazione** e la **formazione**

Priorità di intervento - RDP

- **fornisce**, se richiesto, un **parere** in merito alla **valutazione d'impatto** (art.35)* e ne sorveglia lo svolgimento

- **coopera con l'autorità di controllo**

- **funge da punto di contatto** per l'autorità di controllo per questioni connesse al trattamento

* *DPIA: data protection impact assessment*

Priorità di intervento – Registri delle attività di trattamento

- obbligatorio per tutti i titolari e responsabili, salvo imprese e organizzazioni con meno di 250 dipendenti

- forma scritta, anche in formato elettronico

- a disposizione dell'autorità di controllo su richiesta

Priorità di intervento – Registri delle attività di trattamento

art. 30 e C171

ai fini della redazione del Registro delle attività di trattamento **del titolare** (par.1) è essenziale avviare quanto prima la **ricognizione dei trattamenti** svolti per individuare le principali caratteristiche che andranno poi documentate.

Individuazione di: finalità, categorie di dati e interessati, categorie di destinatari di comunicazione, misure di sicurezza, tempi conservazione e ogni altra informazione utile.

Verifica rispetto principi fondamentali (art.5), di liceità (artt.6, 9, 10), introduzione dei criteri *privacy by design* e *by default* (art.25) – Registro del **responsabile** (par.2)

Priorità di intervento – *data breach*

Notifica di una violazione dei dati all'autorità di controllo (art.33 – C85, C87, C88)

Provvede il titolare nei confronti dell'autorità di controllo, entro 72 ore dall'avvenuta conoscenza, salvo che la lesione ai diritti e delle libertà della persona sia improbabile

Priorità: individuare le idonee procedure organizzative per darvi attuazione

Il Provvedimento n.392 del 2 luglio 2015 prevede 48 ore per le PPAA

… già previsto anche per tlc e fascicolo sanitario

Accountability

Responsabilizzazione

(C74) È opportuno stabilire la responsabilità generale del **titolare** del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto

Titolare (art.4,p.to 7) persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina finalità e mezzi del trattamento dei dati

Accountability

Il titolare decide autonomamente modalità, garanzie e limiti del trattamento del trattamento dei dati …

art. 24 Responsabilità del titolare del trattamento (C74-C78) Mette in atto misure tecniche ed organizzative adeguate per garantire ed essere **in grado di dimostrare** che il trattamento è effettuato conformemente al regolamento

Tenuto conto di natura, ambito di applicazione, contesto, finalità, probabilità e gravità rischi per diritti e libertà persone fisiche

Accountability

Il Regolamento pone con forza l'accento sulla

"responsabilizzazione" di titolari e responsabili

adozione di **comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione dei principi, norme e criteri indicati dal regolamento** (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento)

E' richiesto un approccio sistemico !

Accountability

verifica sui presupposti di liceità del trattamento

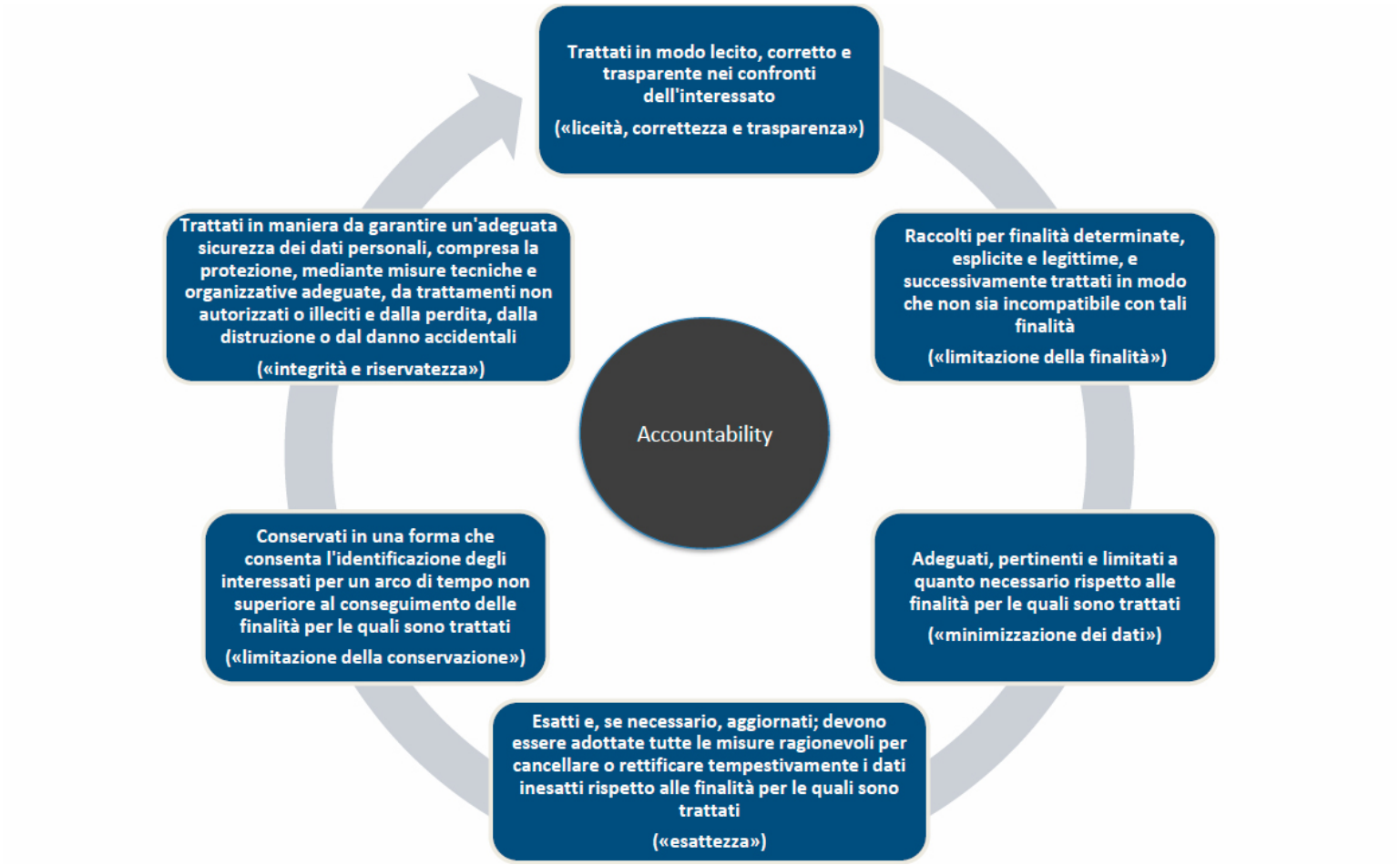
privacy *by design* e *by default* (art.25)

definizione chiara di ruoli e responsabilità

valutazione di impatto (artt. 35 e 36)

Principi applicabili al trattamento

Fonte: Garante



Liceità del trattamento in ambito pubblico

Liceità del trattamento (art.6)

lett. c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento

lett. e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (C45, C46)

art. 9 trattamento di categorie particolari di dati personali

Il trattamento è vietato salvo che sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'UE o degli SM, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (lett. g, C45)

settore della sanità pubblica, finalità di archiviazione nell'interesse pubblico, ricerca scientifica e storica (lett. i, j)

Liceità del trattamento in ambito pubblico

Liceità del trattamento (art.6, par. 3)

La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e) deve essere stabilita dal diritto UE o dello SM

gli SM possono stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri

Liceità del trattamento in ambito pubblico

Liceità del trattamento (art.6, par 3)

Tale base giuridica potrebbe contenere (contiene) disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure attea garantire un trattamento lecito e corretto

Accountability

art.25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

… adozione di misure tecniche ed organizzative che garantiscano il rispetto dei principi di protezione dei dati…

… sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento …

… per impostazione predefinita, dei soli dati necessari per ogni finalità...

privacy by design e *privacy by default*

Individuazione di ruoli e responsabilità

art.26 Contitolari

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento

- definizione, con atto giuridicamente valido, dei rispettivi ambiti di responsabilità e compiti
- gli interessati possono rivolgersi a ciascun titolare
- valutazione attenta di situazioni di contitolarità, indicazione di un punto di contatto per gli interessati

Individuazione di ruoli e responsabilità

art. 28 Responsabile del trattamento

- per i trattamenti svolti per conto del titolare
- scelta su soggetti che assicurino garanzie sufficienti
- trattamenti disciplinati da un contratto (art.28, par.3)
- possibilità di nomina di sub-responsabili, previa autorizzazione scritta del titolare, risponde il responsabile nominato

Obblighi: registro dei trattamenti (art.30, par.2), adozione misure per la sicurezza (art.32), designazione di un RDP (art.37)

Individuazione di ruoli e responsabilità

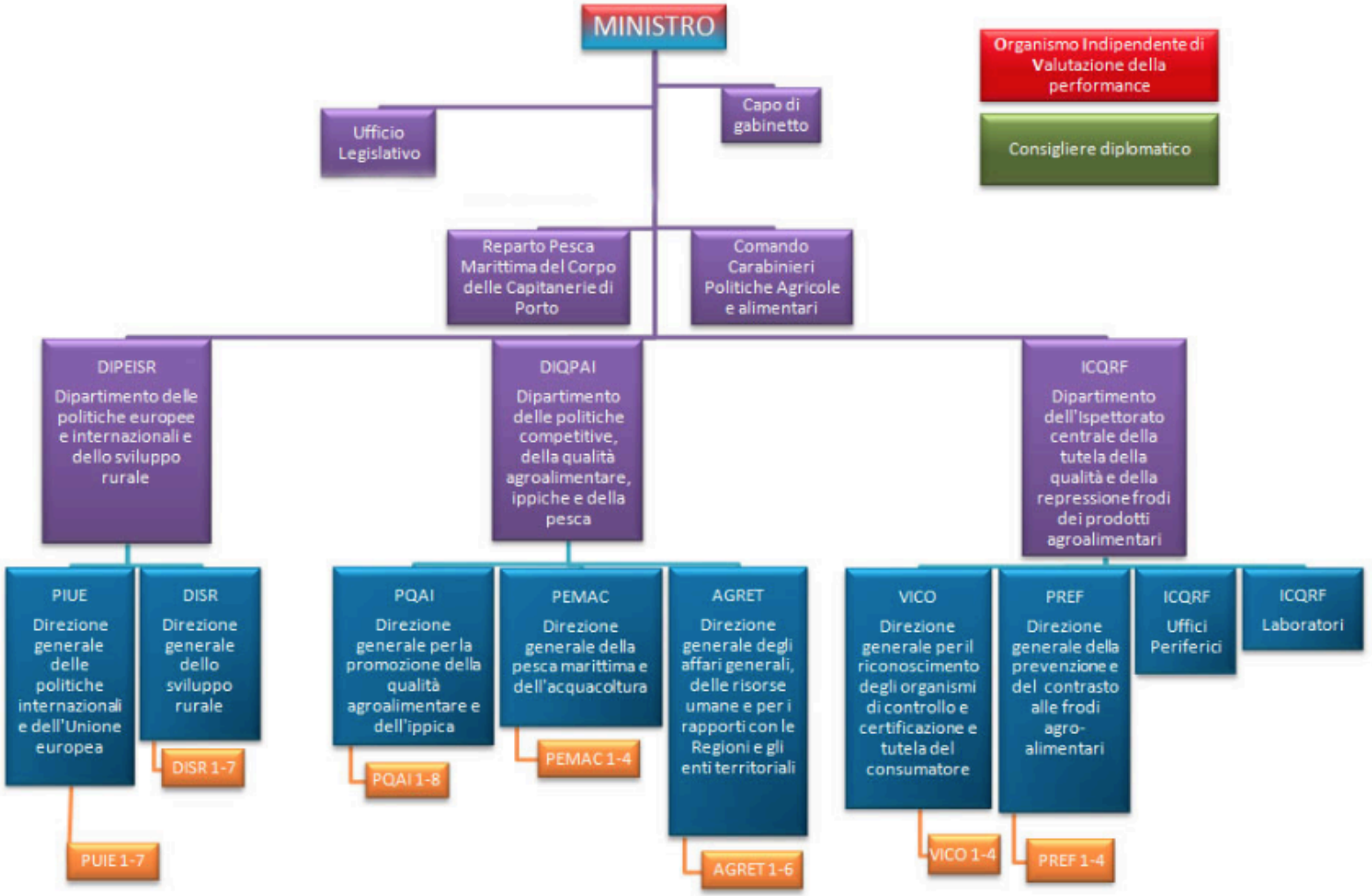
art.4, n. 10 (Incaricati)

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

Garante: designazione opportuna per le PA

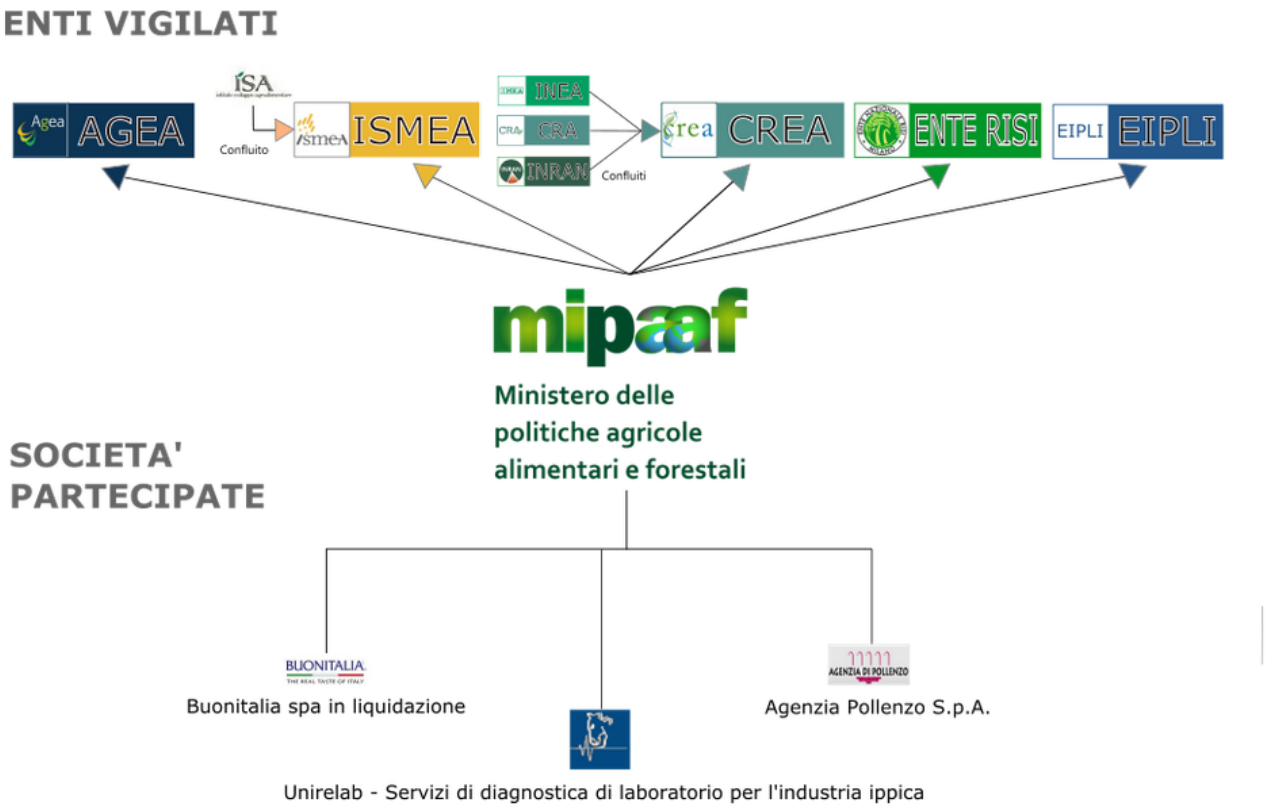
«designazione indispensabile, in quanto permette di considerare legittimo il flusso delle informazioni personali nell'ambito degli uffici e tra i dipendenti dell'amministrazione titolare del trattamento» (nella vigenza della L.675/95)

Organizzazione



Organizzazione

Rappresentazione grafica degli enti vigilati e società partecipate del Ministero



Iniziativa del Garante

dopo l'incontro è stato chiesto un *feedback*
(modulo/questionario)

- cosa è stato fatto? (studio/attività di formazione/atti amministrativi adottati, quali attività in corso)
- quali difficoltà si stanno incontrando rispetto a specifici argomenti?
- come può supportare l'Autorità? Per contribuire a superare problematiche legate al processo di transizione e adeguamento alla nuova normativa
- interesse e disponibilità ad organizzare eventi con l'Autorità?

Banche dati PA servizi - *on line*

Lettera del Presidente del Garante, Antonello Soro, al Presidente Gentiloni su vicenda “Spesometro” e sicurezza banche dati pubbliche (3 ottobre)

GRAZIE PER
L'ATTENZIONE
valelongo72@gmail.com

GRAZIE PER L'OPPORTUNITA'

PROGETTO WINSTON SMITH