ORGANIZZAZIONE, ADEMPIMENTI E ATTORI DEL NUOVO REGOLAMENTO

Michela Massimi

OBIETTIVI

Rafforzamento diritti e doveri

Sburocratizzazione

Uniformità tutele

- Regolamento generale, non Direttiva (v. anche Direttiva 2016/680)
- Proattività titolare / responsabile
- Privacy by design / Accountability
- Sportello unico (One-Stop-Shop)

IN SINTESI:

- **«Accountability»**
  - **proattività**: approccio basato sul rischio del trattamento
  - **privacy by design/default**
  - **valutazione di impatto**
  - **RPD**
  - **registro dei trattamenti**
  - **certificazione trattamenti/codici di condotta**
- **Nuovi diritti interessati**: «oblio», limitazione, portabilità
- **Ruolo Autorità di controllo**: «sportello unico» e meccanismo di coerenza
- **Sistema sanzionatorio**: sanzioni tendenzialmente uniformi in Ue

ACCOUNTABILITY

parole chiave **Responsabilizzazione** **Rischio**

- Obbligo incombente su titolari
- **Fattori da considerare**: natura, ambito, contesto, finalità del trattamento + rischi per diritti e libertà fondamentali dell'interessato
- **Risultato**: misure tecniche e organizzative adeguate
- **Obiettivo**: garantire ed essere in grado di dimostrare compliance ➔ Documentabilità dei processi
- Permanente, non una tantum

ACCOUNTABILITY

Strumenti e obblighi

privacy by design/by default	(art. 25)
misure di sicurezza	(art. 32) adeguate, in base al rischio, per obiettivi (riservatezza, integrità, disponibilità, resilienza) + processo di revisione continua ➔NO MISURE «MINIME»
valutazione di impatto privacy	(artt. 35-36) trattamenti a rischio elevato - consultazione preventiva Autorità ➔ NO AUTORIZZAZIONE PREVENTIVA
designazione di un RPD	(artt. 37-39) criteri nomina, requisiti soggettivi, compiti (vigilanza DPIA, interfaccia con Autorità e interessati)
codici di condotta/certificazione trattamenti	(artt. 40-43) strumenti per dimostrare compliance

ACCOUNTABILITY

Strumenti e obblighi

Contitolari e responsabili del trattamento

(artt. 26, 28) disciplina della contitolarità e rafforzamento obbligo di garanzie contrattuali fra titolare e responsabile (che può nominare direttamente sub-responsabili)

Registro delle attività di trattamento

(art. 30) importante ai fini della gestione protezione dati (esenzioni per PMI < 250 dipendenti)

Data breach

(artt. 33, 34) notifica violazioni di dati ad Autorità/agli interessati (criteri di soglia basati sul rischio)

ATTORI E RUOLI

- Titolare del trattamento
- Contitolare del trattamento
- Responsabile del trattamento
- Persone autorizzate al trattamento
- Responsabile della protezione dei dati

TITOLARE

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le **finalità** e i **mezzi** del trattamento di dati personali *(art. 4, par. 7)*

CONTITOLARE

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

(art 26)

CONTITOLARITÀ

La disciplina della **contitolarità del trattamento** impone ai titolari di definire specificamente il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari che operano congiuntamente

- I contitolari determinano con **accordo interno** le rispettive responsabilità in merito all'osservanza degli obblighi, all'esercizio dei diritti dell'interessato e all'informativa
- L'accordo interno (nel contenuto essenziale) è messo **a disposizione degli interessati**

RESPONSABILE DEL TRATTAMENTO

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto del titolare** del trattamento

(art. 4, par. 8; art. 28)

RESPONSABILE DEL TRATTAMENTO

Il responsabile **può nominare sub-responsabili** per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e «responsabile primario»

Il «responsabile primario» **risponde dinanzi al titolare dell'inadempimento del sub-responsabile** anche ai fini del risarcimento di eventuali danni causati dal trattamento

RESPONSABILE DEL TRATTAMENTO

Necessità di un **contratto** (o altro atto giuridico) che disciplini:

- materia e durata del trattamento;
- natura e finalità del trattamento;
- tipo di dati personali e categorie di interessati;
- obblighi e diritti del titolare del trattamento.

RESPONSABILE DEL TRATTAMENTO

In base al **contratto** il responsabile si impegna a:

- trattare dati soltanto su istruzione documentata del titolare;
- consentire i trattamenti **solo a persone autorizzate** con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure di sicurezza (es. cifratura; pseudonimizzazione; recupero da backup);
- rispettare le condizioni per ricorrere a un sub-responsabile del trattamento;
- assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- **cancellare o restituire** tutti i dati e cancellare le copie esistenti;
- mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.

RESPONSABILE DEL TRATTAMENTO

- La **Commissione** può stabilire **clausole contrattuali tipo** per le materie oggetto del contratto tra titolare e responsabile

- L'**autorità di controllo** può adottare **clausole contrattuali tipo** per le materie oggetto del contratto tra titolare e responsabile, in conformità del meccanismo di coerenza di cui all'articolo 63

PERSONE AUTORIZZATE

È definito «**terzo**» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che non sia la persona autorizzata** al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

(art. 4, par. 10)

TRATTAMENTO SOTTO L'AUTORITÀ DEL TITOLARE O DEL RESPONSABILE *(art. 29)*

Il responsabile del trattamento, o **chiunque** agisca sotto la sua autorità o sotto quella del titolare del trattamento, che **abbia accesso** a dati personali **non può** trattare tali dati **se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

SICUREZZA DEL TRATTAMENTO
(art. 32, par. 4)

Il titolare del trattamento e il responsabile del trattamento fanno sì che **chiunque** agisca sotto la loro autorità e **abbia accesso** a dati personali non tratti tali dati **se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

RESPONSABILE DELLA PROTEZIONE DEI DATI
(art. 37, 38, 39; cons. 97)

La designazione del RPD è obbligatoria se:

- il trattamento è effettuato da **autorità pubbliche o organismi pubblici**

  (eccezione: Autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali)

- si svolgono trattamenti su **larga scala**
  - monitoraggio regolare e sistematico degli interessati
  - categorie particolari di dati personali (art. 9) e dati relativi a condanne penali e a reati (art. 10)

v. "*Linee guida sui Responsabili della Protezione dei Dati (RPD)*" del 13 dicembre 2016, del "Gruppo di lavoro art. 29", WP 243 rev. 01Linee guida 5 aprile 2017

RESPONSABILE DELLA PROTEZIONE DEI DATI

Designazione per più titolari

Più autorità pubbliche o organismi pubblici possono designare un **unico RPD** tenuto conto delle dimensioni e della struttura organizzativa

(art. 37, par. 3)

RESPONSABILE DELLA PROTEZIONE DEI DATI

Requisiti richiesti

- **Qualità professionali** (esperienza professionale, formazione specialistica, certificazioni, etc.)
- **Conoscenza specialistica -** Normativa e prassi in materia di protezione dati **-** Disciplina di settore
- **Capacità di assolvere i compiti previsti**
- **Autonomia e assenza di conflitto di interessi**

RESPONSABILE DELLA PROTEZIONE DEI DATI

Interno

Dipendente del titolare

Esterno

Contratto di servizio (professionista o società di consulenza)

GRAZIE PER L'ATTENZIONE

Michela Massimi