Adeguamento al GDPR: priorità e suggerimenti

Venezia, 14 novembre 2017

Cambia l'approccio

Approccio molto orientato agli adempimenti formali

(misure minime; designazioni; ecc)

Approccio basato sul principio di responsabilizzazione (c.d. «accountability»)

- Garantire il rispetto dei principi del GDPR
- Essere in grado di dimostrare di aver messo in atto misure tecniche e organizzative dimostrandone l'efficacia in relazioni ai rischi sottesi al trattamento

Tempi per adeguamento

- Nuovi adempimenti e intensa attività di adeguamento, preliminare alla sua definitiva applicazione a partire dal 25 maggio 2018.

Priorità per le PA

- Nomina del responsabile della protezione dei dati personali
- Istituzione del registro delle attività di trattamento
- Notifica di violazioni dei dati personali all'autorità di controllo

Priorità per le PA

- Nomina del responsabile della protezione dei dati personali (RPD)
- Istituzione del registro delle attività di trattamento
- Notifica di violazioni dei dati personali all'autorità di controllo

Data Protection Officer (DPO)

Il DPO (artt. 37-39)

- facilita l'osservanza delle disposizioni del GDPR
- è una figura obbligatoria se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. La direttiva 95/46/CE non prevedeva alcun obbligo di nomina del DPO, ma in molti Stati dell'UE questa era divenuta una prassi nel corso degli anni
- può essere interno o esterno [in entrambi i casi non risponde personalmente in caso di inosservanza del GDPR da parte del titolare o del responsabile].

Individuazione del DPO (1/2)

In proporzione alla sensibilità, complessità e quantità dei dati trattati e alla tipologia di ente:

- È possibile designare un unico DPO per più autorità pubbliche
- È richiesto uno specifico livello di conoscenza specialistica

Il DPO è individuato in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati

Individuazione del DPO (2/2)

- tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali
- dotato di risorse necessarie per assolvere ai compiti e mantenere la conoscenza specialistica
- con compiti e funzioni che non devono dare adito a un conflitto di interessi.

Cosa fare

- Effettuare la nomina, eventualme
  esplicitando le modalità per prevenire casi di conflitto di interessi.
- Comunicare i dati di contatto del DPO all'autorità di controllo
- Pubblicare i dati di contatto del DPO

Cosa fare

Definire con il DPO

un ordine di priorità per concentrarsi sugli ambiti che presentino rischi più elevati e sui casi nei quali risulti necessario effettuare la valutazione di impatto (DPIA)

DPIA

Il regolamento fissa le caratteristiche basilari di una DPIA all'art. 35, paragrafo 7, e nei considerando 84 e 90:

- "una descrizione [sistematica] dei trattamenti previsti e delle finalità del trattamento";
- "una valutazione della necessità e proporzionalità dei trattamenti";
- "una valutazione dei rischi per i diritti e le libertà degli interessati";
- "le misure previste per:
  - o "affrontare i rischi";
  - o "dimostrare la conformità con il presente regolamento". "

Priorità per le PA

- Nomina del responsabile della protezione dei dati personali
- Istituzione del registro delle attività di trattamento
- Notifica di violazioni dei dati personali all'autorità di controllo

Registro trattamenti

Istituzione del Registro delle attività di trattamento (art. 30 co.1)

- Ricognizione dei trattamenti svolti e delle principali caratteristiche
  - Finalità del trattamento
  - Categorie di dati e interessati
  - Categorie di destinatari cui è prevista la comunicazione
  - Eventuali trasferimenti verso paesi terzi (con documentazione delle garanzie adeguate)
  - Tempi di conservazione
  - Misure di sicurezza tecniche e organizzative

Caratteristiche del registro

- Strumento di verifica dei principi e delle misure a protezione dei dati
- Forma scritta (anche in formato elettronico)
- A disposizione dell'autorità di controllo
- Previsto l'obbligo di un registro separato anche per il Responsabile del trattamento

Da dove partire…

Un gruppo di lavoro CODAU ha:

i. Stilato una lista dei trattamenti comuni agli Atenei per redigere una bozza delle attività di trattamento
ii. Prodotto un documento di linee guida, sottoponendo all'Autorità Garante alcuni dubbi interpretativi che riguardano gli Atenei
iii. Organizzato alcuni incontro per confrontare e analizzare alcune soluzioni digitali per il registro presenti sul mercato

Cosa fare

- Formazione
- Individuazione dei trattamenti e di una soluzione per la tenuta del registro
- Individuazione delle responsabilità per la tenuta e aggiornamento del registro
- Analisi dei rischi in relazione ai trattamenti mappati e individuazione di azioni per adeguamento al GDPR

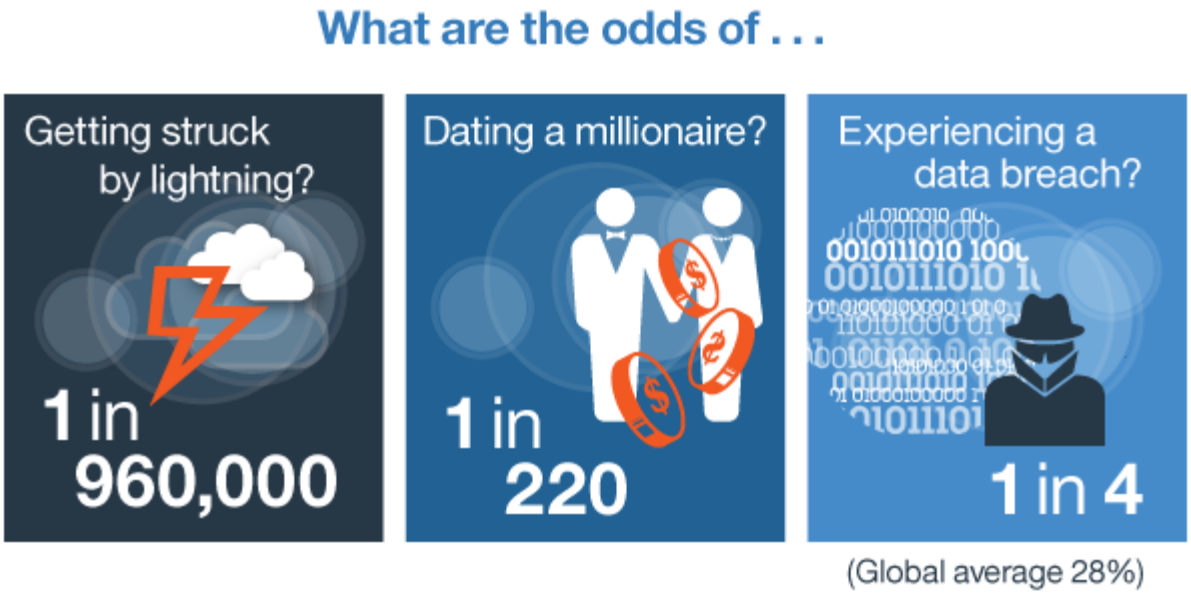
Priorità per le PA

- Nomina del responsabile della protezione dei dati personali
- Istituzione del registro delle attività di trattamento
- Notifica di violazioni dei dati personali all'autorità di controllo

Data breach **(artt. 33 e 34)**

«Violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»

Inquietanti statistiche



Il rischio è quello di essere una Ferrari con le gomme lisce!

Cambia l'approccio

I panni sporchi non si lavano più in famiglia!

Pensiamo alle campagne di richiamo delle case costruttrici di automobili:

l'intesse è salvaguardare il rapporto di fiducia tra costruttore d'auto e acquirente finale

Data Breach

Notifica delle violazioni dei dati personali all'autorità di controllo

- senza ingiustificato ritardo
- al massimo entro 72 ore dal momento in cui il Titolare ne viene a conoscenza.

Se la violazione è suscettibile di presentare un rischio elevato per l'interessato, l'interessato deve essere informato (salvo il titolare non abbia adottato misure preventive come la *cifratura*)

Contenuti della notifica

Il titolare del trattamento documenta qualsiasi violazione dei dati personali

- Natura della violazione (ove possibile, indicando le categorie e il numero approssimativo di interessati)
- Nome e dati di contatto del DPO o di altro punto di contatto;
- Probabili conseguenze della violazione;
- Misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali o attenuarne i possibili effetti negativi.

Cosa fare

- Individuazione di misure di prevenzion
- Redazione di procedure specifiche su come comunicare le violazioni (a Garante e/o interessato)
- Individuazione misure da adottare per attenuare gli effetti negativi della violazione
- Definizione delle caratteristiche delle violazioni suscettibili di presentare un «rischio elevato»

Altri aspetti importanti

- Formazione a tutti i livelli
- Aggiornare policy interne in materia di protezione dei dati personali
- Prestare maggiore attenzione a impostare (almeno) i nuovi trattamenti nella logica della «privacy by design» e «privacy by default»
- Analisi delle responsabilità (responsabili esterni; delega di compiti agli attuali Responsabili del trattamento)

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Manuela Zecca

Area Sistemi Informativi e Applicazioni

privacy@unibo.it

www.unibo.it