Il GDPR nella mia azienda: la visione degli esperti e il confronto con le aziende

Tavola Rotonda della Oracle Community for Security con la collaborazione di Europrivacy e Clusit

Modera Alessandro Vallega - Oracle, Europrivacy, Clusit


17 marzo 2015 – Security Summit Milano
Plenaria GDPR con il Presidente Antonello Soro; Clusit


17 gennaio 2017 – Osservatorio Information Security e Privacy
Con il patrocinio di Aused, Clusit e Europrivacy
Plenaria GDPR con il dott. Casel

15 marzo 2018 – Security Summit Milano
Plenaria con Gabriele Faggioli e video di Giovanni Buttarelli (https://clusit.it/clusit-incontra-le-istituzioni/)

7 giugno 2018 – Security Summit Roma / il GDPR è applicabile
TR con il patrocinio di Oracle Community for Security, Europrivacy, Clusit e Aused
Siamo ancora tutti qui...

E cosa abbiamo fatto nel frattempo?
Cosa stiamo facendo?
Cosa ci manca?

Per rompere il ghiaccio rispondiamo ad una survey

- Ci sono 13 semplici domande
- Le prime riguardano il settore merceologico e la dimensione d'impresa
- Le altre 11 aspetti specifici del GDPR che dovrebbero essere implementati in azienda (li vediamo tra un attimo).
- Ad ognuna bisogna rispondere
  - Non rispondo, non so o non applicabile
  - L'azienda in considerazione l'avrà fatto entro il 25/5 (o l'ha già fatto)
  - L'azienda in considerazione sa che dovrebbe, ma non l'avrà fatto entro il 25/5
  - L'azienda in considerazione non lo farà perché non ritiene di doverlo fare
- Si deve rispondere se si conosce abbastanza bene l'azienda in considerazione
- Si può rispondere alla survey più volte per enne aziende che si conoscono

Le 11 domande riguardano

1. assegnare il ruolo di DPO
2. rivedere policy e procedure
3. rivedere i contratti di fornitura
4. rivedere la / le informative agli interessati
5. modificare le applicazioni e le procedure per rispettare i criteri di minimizzazione e conservazione limitata nel tempo
6. modificare le applicazioni e le procedure per i diritti dell'interessato di accesso, all'oblio, alla portabilità
7. ristrutturare la gestione del consenso (raccolta e uso appropriato dello stesso)
8. creare i registri delle attività di trattamento
9. preparare le procedure per la notifica della violazione dei dati personali al Garante
10. preparare le procedure per la comunicazione della violazione dei dati personali agli interessati
11. adottare misure di sicurezza aggiuntive rispetto alla situazione precedente all'approvazione del GDPR

Per favore compilatela anche voi adesso con il vostro cellulare

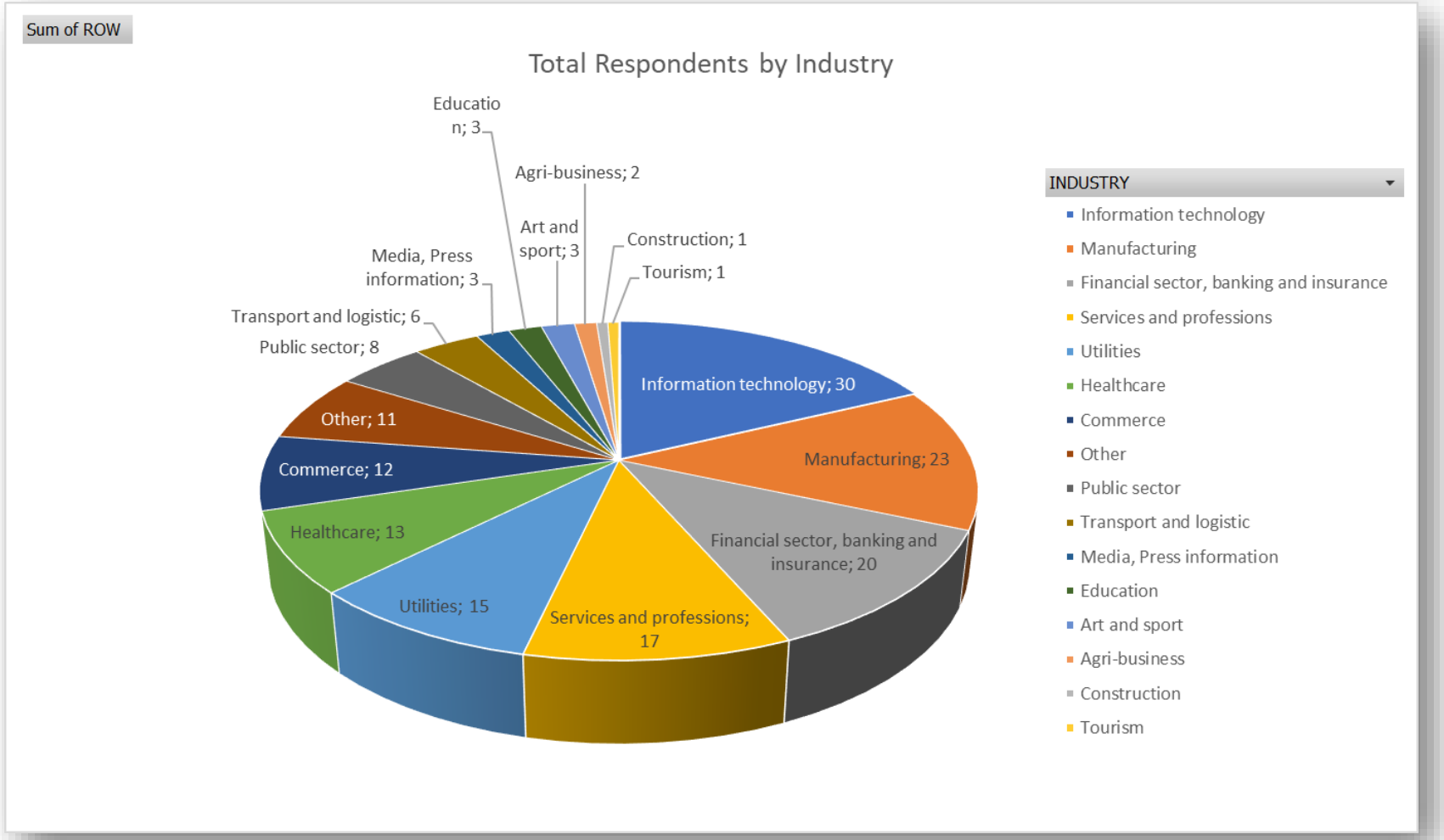
https://survey.clusit.it/C4S-GDPR

GDPR Survey

168 risposte per 16 *industry*

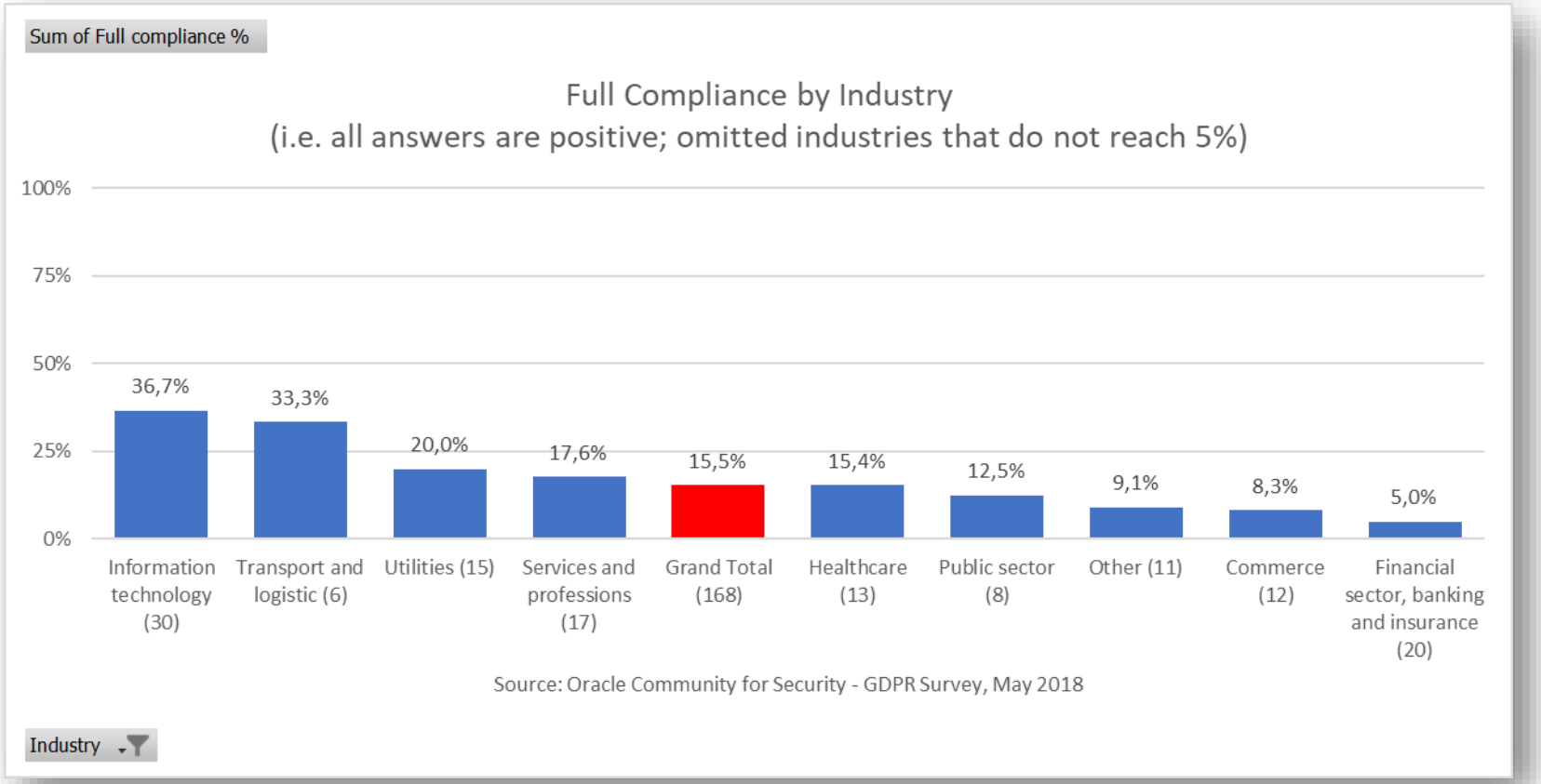
Dati raccolti in marzo e maggio in Italia

La survey è stata estesa all'Europa, Medio Oriente e Africa e sarà aggiornata regolarmente



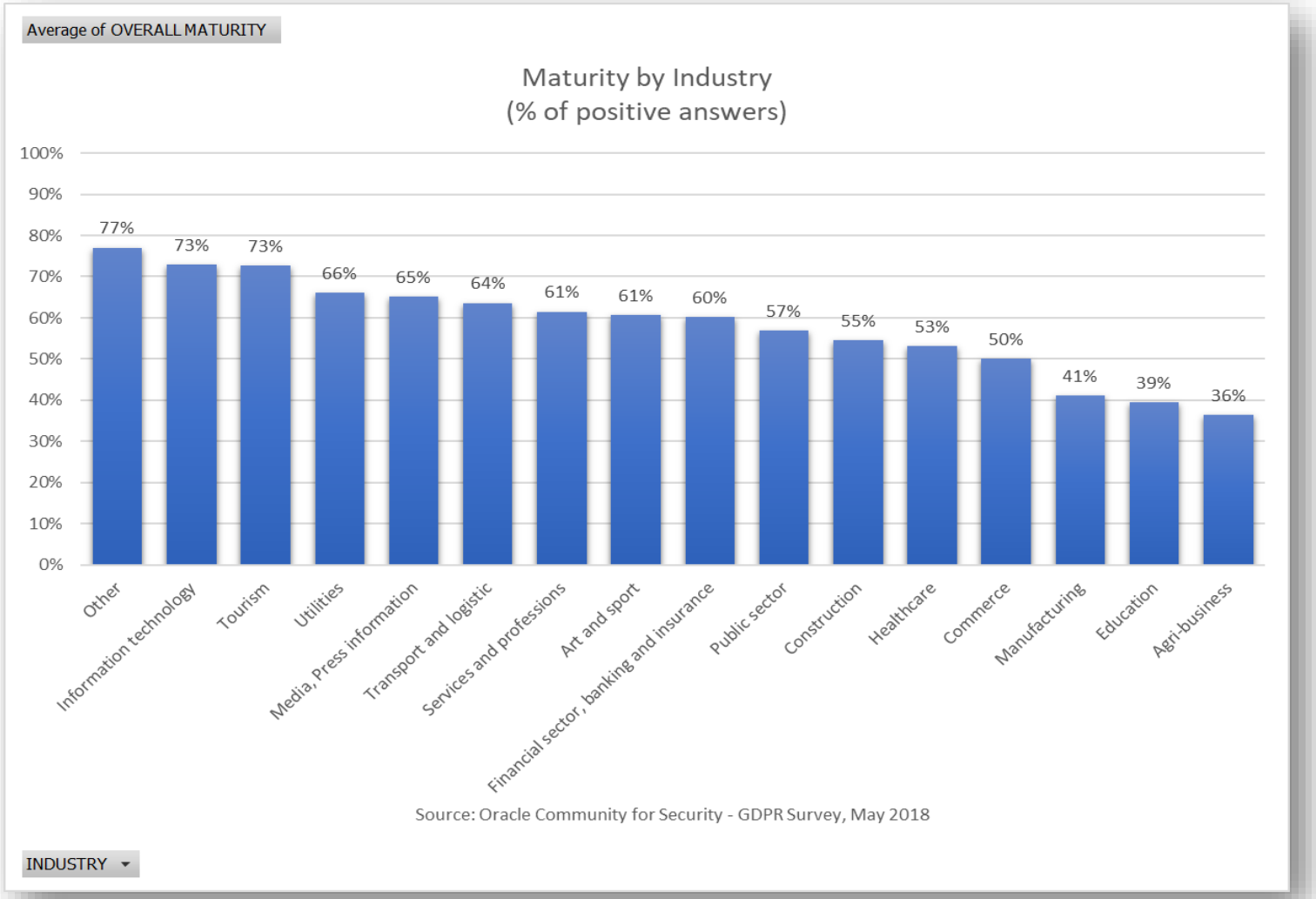
GDPR Crisp Compliance

Se il GDPR è un viaggio, c'è ancora molta strada da fare...



Nota: crisp compliance o full compliance, significa che tutte le domande hanno avuto risposta positiva (o non applicabile all'azienda).

GDPR Maturity by Industry



La situazione migliora se valutiamo la percentuale di risposte positive; comunque la maggior parte delle *industry* non raggiunge il 60% di esse

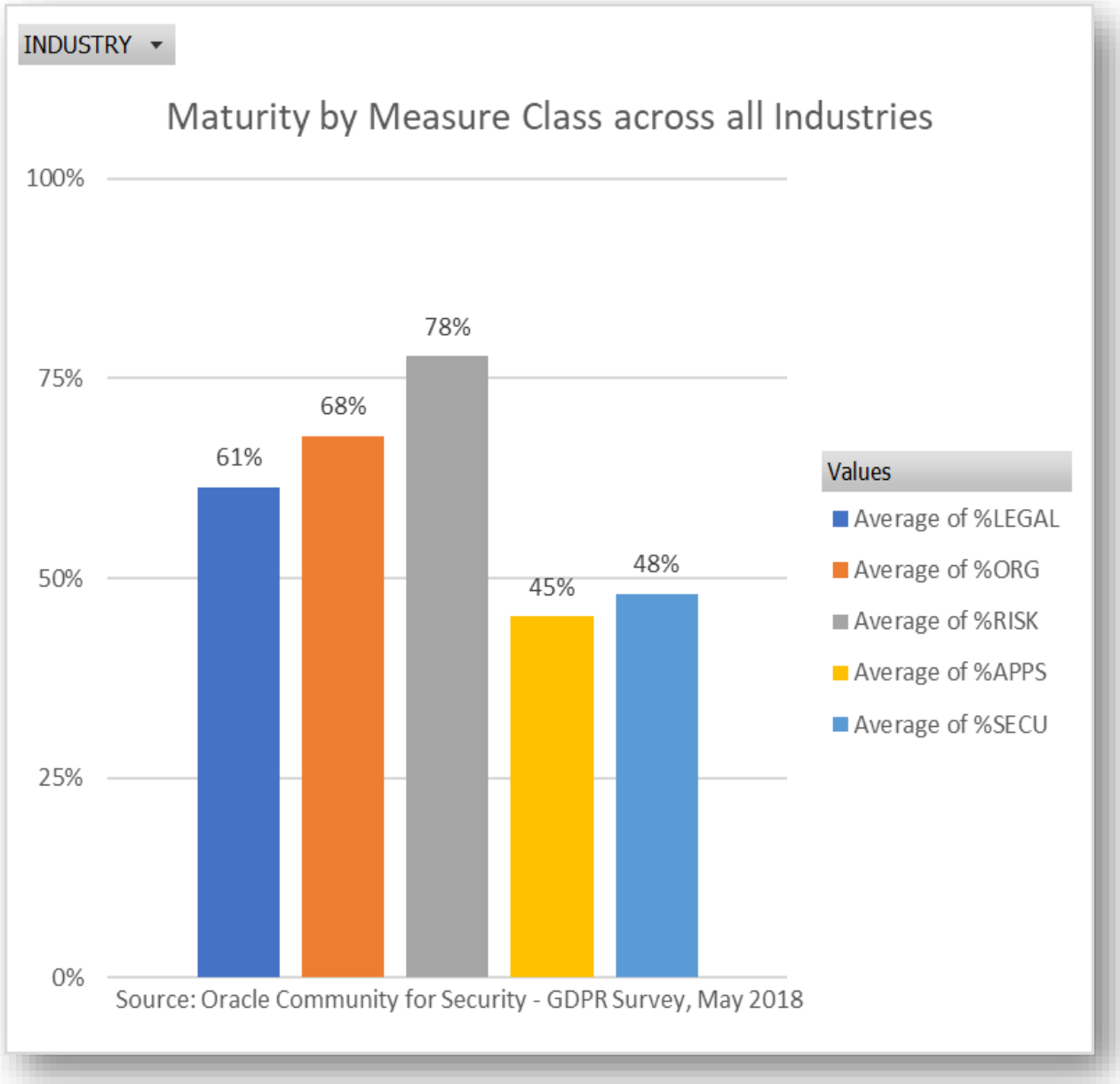
Maturity by Class

Tipi diversi di misure hanno gradi di maturità differente.

Si osserva una maggior maturità per la classe «RISK», per via del fatto che molti progetti GDPR sono partiti con il registro dei trattamenti (art. 30)

I progetti relativi a «APPS» sono molto complessi nelle organizzazioni complesse caratterizzate da sistemi informativi stratificati negli anni e dotati di molti *custom*

I progetti «SECU» non sono necessariamente molto complessi ma sono partiti tardi.



Vediamo cosa avete risposto...

Comparazione tra i dati precedenti e quelli raccolti adesso...

Riprendiamo la discussione... Chi sono i nostri esperti

FABRIZIO BULGARELLI
RSM ITALY

GABRIELE FAGGIOLI
CLUSIT – P4I

FRANCESCO GRASSO
(UMBERTO PRIMO)

STEFANO MONI
POLIZIA DI STATO

NICOLA PAOLINO
KPMG

MARCO SIMONCINI
ENAV

Regole della discussione
- E’ possibile dissentire con il moderatore (e gli altri)

Spunti per iniziare
- I dati della survey hanno sorpreso?
- Suggerimenti per chi non ha ancora finito il viaggio
- Lessons learned

Gabriele rompe il ghiaccio

Ringraziamenti e prossime azioni

Se è interessato a ricevere, quando pronto, un report di analisi della survey per favore scriva un email a securityCommunity_it@oracle.com

Manifesto di Europrivacy

- Europrivacy.info è un blog collettivo, che nasce nel 2015 da un'iniziativa di Aused, di Clusit e di Oracle Community for Security, di professionisti esperti in Sicurezza e Compliance che vogliono contribuire allo sviluppo della consapevolezza delle organizzazioni in merito al nuovo Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679) e alle norme europee collegate.
- Il punto di vista che si propone di esprimere è multidisciplinare e si realizza grazie al lavoro di contributori provenienti sia dal mondo *Legal* sia da quello dell'*Information Technology.* Il blog ha l'obiettivo di diventare un punto di riferimento nel percorso di adeguamento alla nuova normativa e di contribuire al dibattito internazionale, di conseguenza i post sono tradotti in inglese.

Europrivacy.info @europrivacy