considerazioni su GDPR vs FLOSS

Autore Giovambattista Vieri (ENT SRL)

introduzione

- La presentazione è pensata per persone con interessi tecnici e non.
- Non si useranno termini tecnici informatici ma, per forza di cose si riporteranno dei virgolettati.
- Si comincerà a delineare il campo per poi arrivare alle conclusioni con dei possibili impatti sugli sviluppatori floss (e magari SME)

Dati personali

- Proviamo a definire “dati personali” secondo la nuova normativa:
  - Dati sensibili come finanza, salute, patrimonio genetico
  - Ma anche Ip (address)
  - Tutto ciò che ha a che fare con una “natural person”
- punto 51 pag 31
- Articolo 6 4 a pag 122 :

Dati Personali

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Dati non soggetti alla GDPR

- Dati anomizzati/pseudo anomizzati
- Dati che ragionevolmente non possono essere ricondotti a “dati di natural persons” (pt 26 p.16)

RAGIONEVOLMENTE

In passato ciò che era ragionevolmente non riconducibile a … lo diventava tipicamente dopo un anno … Vedremo …

Bambini

Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

Punto 38 p 17

GDPR

- E' una direttiva UE... dovrà essere recepita entro due anni negli stati membri della UE.

A chi non si applica?

- This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity.
- “by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data,”
- Ai dati di persone decedute

CHI NON DEVE APPLICARLA?

- Articolo 30 ch IV …
- Sicuramente chi ha meno di 250 dipendenti e, non è coinvolto nel business della profilazione dei dati... e non processa categorie speciali di dati...

FLOSS

- E' un termine usato per la prima volta dalla UE nel 2001
- FL Free/Libre/Liber etc.
- Open Source Software
- L'uso del termine si diffonde sempre di più...

Intermezzo

- Il testo della GDPR è un pdf.
- Si trasforma facilmente in txt (formato testo) con pdftotxt (linux)
- Poi con python e https://github.com/wheatear/wordsworth è velocissimo fare qualche analisi

Statistico
2 parole

- 4 = the controller (339 = 0.618%)
- 5 = in the (326 = 0.594%)
- 6 = supervisory authority (325 = 0.593%)
- 7 = the data (302 = 0.551%)
- 8 = this regulation (294 = 0.536%)
- 9 = of personal (284 = 0.518%)

3 parole

- 6 = the data subject (214 = 0.390%)
- 7 = the personal data (135 = 0.246%)
- 8 = the processing of (129 = 0.235%)
- 9 = the supervisory authority (129 = 0.235%)
- 10 = in accordance with (122 = 0.222%)
- 11 = processing of personal (118 = 0.215%)
- 12 = of this regulation (113 = 0.206%)
- 13 = the controller or (110 = 0.200%)
- 14 = controller or processor (106 = 0.193%)

4 parole

- 3 = processing of personal data (118 = 0.215%)
- 4 = the processing of personal (94 = 0.171%)
- 5 = referred to in article (88 = 0.160%)
- 6 = referred to in paragraph (72 = 0.131%)
- 7 = the controller or processor (71 = 0.129%)
- 8 = union or member state (66 = 0.120%)
- 9 = rights and freedoms of (62 = 0.113%)
- 10 = or member state law (62 = 0.113%)
- 11 = of the data subject (61 = 0.111%)
- 12 = to the processing of (52 = 0.094%)

Fine intermezzo

- Pare chiaro di cosa si parla
- Son importanti processor e controller
- Di più “dati personali”
- Ma anche “l'autorità di supervisione” …

Considerazioni sulla GDPR

- E' una direttiva che deve essere recepita nelle legislazioni degli stati membri.
- Sostituisce le direttive precedenti
- Quindi possiamo immaginare che le leggi che ne deriveranno sostituiranno le leggi precedenti

Struttura

- Divisa in articoli
- Raggruppati in Chapter
- Gli articoli si dividon in paragrafi/punti

struttura

1) General Provisions
2) Principles
3) Rights of the Data Subject
4) Controller and Processor
5) Transfer of personal data to third countries of international organizations
6) Independent Supervisory Authorities

struttura

7) Co-operation and consistency
8) Remedies, Liability, and Sanctions
9) Provisions relating to specific data processing situations
10) Delegated Acts and Implementing Acts
11) Final provisions

struttura

- Degni nota 3 4 6 7
- Il “capitolo” sanzioni può essere pesante... % del fatturato globale …

Qualche termine

- Controller
  - is anyone who determines the “purposes and means of processing of the personal data.”
- Processor
  - Chi processa I dati per conto o per il controller
- Dpo
  - Data Protection Officer … una figura che diventerà obbligatoria nelle aziende impattate dai vari “recepimenti nazionali” e dovrà cooperare con le varie DPA (data protection agency) riferendo al massimo livello di management e senza svolgere compiti in contraddizione

Argomenti scelti

- A chi si applica
- Consenso (al trattamento)
- Data breach
- Privacy by design
- Right to access/be forgotten / Data portability

A chi si applica?

- A tutti coloro che in un modo o in un altro abbiamo a che fare con dati personali di cittadini UE.
- Siano essi controller o processor.
- Siano le eventuali transazioni economiche correlate in effetuate in ue o meno

Consenso al trattamento

- La richiesta di consenso deve essere in termini chiari ed espliciti
- Altrettanto chiare ed esplicite la finalità
- Esplito l'accettazione (no ad azioni impliciti come scorrere la pagina)
- Consenso tracciato

Esempi/link

- Articoli 40 42 (il controller deve dimostrare...)
- 43 (granularità del consenso)
- 44 (casi di contratti) 45 processamento per obblighi di legge 46/50 “eccezione” per condizioni di pericolo di vita o altre “eccezionalità”

Data breach

- Ohi ohi ohi
- Và notificata entro 72 ore.
- Il processor deve avvertire il controller e poi ambedue devono avvertire le persone coinvolte.
- Il tempo scatta dal momento in cui ci si accorge della “breach”

Ma cosa è una “data breach”?

- Perdita di dati personali (sì anche cancellazione)
- Diffusione non autorizzata di dati personali
- Dispersione non autorizzatata di dati personali
- Uso improprio degli stessi (anche all'interno della stessa organizzazione)

considerazioni

- Milioni di dollari di sanzioni + % del fatturato
- Il dpo collabora con l'autorità
- Coloro che sono descritti dai dati devono essere avvertiti
- …..
- …
- .

Privacy by design

- BASTA CON UNA UNICA TABELLA PER USERNAME PASSWORD E ANAGRAFICA COMPLETA FINO ALLA 7 GENERAZIONE!
- Scherzi a parte, non è cosi facile. Ma di certo da ora in poi le anagrafiche dovran essere trattate con più rispetto e meno accessibili all'interno delle applicazioni.

Privacy by Design

- http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2015-04-20/privacy-by-design-approccio-corretto-protezione-dati-personali-123915.php
- https://it.wikipedia.org/wiki/Privacy_by_design
- https://blog.varonis.com/privacy-design-cheat-sheet/
- L'ultimo link è un cheat sheet … rapido e veloce...
-

Privacy by design

- La direttiva indica che la crittografia e codifiche varie possono essere usate per mitigare il/i problemi derivanti da vecchie architetture o, ereditati da vecchi applicativi.
- E' evidente che molto lavoro di analisi dovrà essere compiuto sulle applicazioni Legacy.

•Right to access/be forgotten / Data portability

- Articolo 65 pag 39

Articolo/i

- 81 (processors certificati)(p.50)
- 83 (crittografia) (p.51)
- 63 (segreti commerciali nel software) che non dovrebbero impedire la “consegna” dei dati utente … (p.38)

Alla fin fine

- Sicuramente ignorare la direttiva, o meglio le leggi e regolamenti che ne derivano può esser costoso
- Sicuramente la privacy và tutelata
- In funzione di come verrà recepita la direttiva SME e sviluppatori FLOSS subiranno impatti
- Un sistema conforme di Single Sign On potrebbe salvare privacy FLOSS e business ?

In ogni caso

- Gli obblighi sui controller processor si ripercuoteranno
  - sulla “chain-value” del software development (uso di crittografia, tabelle anagrafiche che non coincidono con quelle di login etc)
  - Sulle licenze e sui contratti.. Quindi anche sulle licenze libere
  - Forse la figura dello sviluppatore indipendente per certe “lavorazioni” dovrà modificare il business model

innovazione

- Molte innovazioni son nate negli ultimi tempi con lo scopo di trattare sempre più dati sempre più velocemente. Ora l'innovazione dovrà tener conto di nuove condizioni al contorno.
- Questo si applica anche tutte quelle nuove aziende che hanno un Business Model incentrato su dati prodotti e diffusi dagli utenti

Auspici

- Speriamo di non:
  - vedere n (con n che tende al numero degli stati UE) normative solo apparentemente simili
  - Vedere aumentare le liti tra aziende (processor/controller) e utenti
  - Rallentare il tasso di innovazione/sviluppo economico
- Speriamo di assistere allo sviluppo di una maggiore consapevolezza dell'importanza dei dati personali sia tra gli utenti sia tra le aziende.

Conclusioni

- Difficili fino al recepimento nelle normative nazionali
- Di certo lo sviluppo software dovrà inserire nuovi constraint nelle specifiche (criptografia dei dati personali) e nel disegno delle basi dati
- Le SME dovranno fare attenzione a limiti e opportunità introdotte dalla normativa
- Alcuni consulenti si riconvertiranno
- Gli impatti economici non saranno trascurabili