CBPL
Commissie voor de bescherming van de persoonlijke levenssfeer

CPVP
Commission de la protection de la vie privée

CPP
Commission for the protection of the privacy

ASP
Ausschuss für den Schutz des Privatlebens

Smart metering and European data protection law

19 April 2012

Content

1. DP Opinions
2. Known DP Risks
3. points of attention in present & future DP regulatory framework
4. Practical recommendations
5. Conclusion

1. DP Opinions

- Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Convention 108)

  https://wcd.coe.int

- WP 29 Opinion 12/2011 of 4 April 2011 on smart metering (hereafter "WP 183 ")

  http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

1. DP Opinions

- WP 29 Opinion 04/2007 ("WP 136") on concept of personal data

  http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm

2. Known DP risks

- ≠ in MS due to Energy & DP Directives : different legal language ex : "third parties" vs. ESCO's, "purposes" vs. Functionalities ("**tower of babel**")
- Margin of interpretation of Directives ⇨ risk of unbalanced approach (risk of "**goldplating**")
- EC smart grid targets impact on legitimate processing grounds (article 7 DP Directive). If free consent not possible for basic roll-out : shifts more weight to **quality** of laws and contracts (8 ECHR)
- Different actors & complex network & tasks ⇨ need to ID who the data controller is for what processing operation (risk of lack of **accountability**)?

2. Known DP risks

- Lack of study and attention on impact of future uses of energy profiles (energy load graphs) and related unqiue EAN data for law enforcement, "scientific" research, deep packet inspection applied to smart grid data, multisectoral profiling for debt assessment of consumers (consumer credit + telcom + energy data) ⇔ smart grids as a development "towards greater consumer empowerment" ? (**top of the functionalities iceberg**)
- Current lack of multidisciplinary view ⇔ p18 WP 183 and EC Rec 2012/148/EC of 9 March 2012) ("**wearing blinkers**")
- "independent" data management⇔ DSO enters the ESCO market (risk of **function creep** ?)

3. Points of attention

Recital 5 Commission Recommendation 2012/148/EU of 9 March 2012 (OJ 13 March 2012, L 73/9) :

DP is a key task and a condition precedent for roll-out

"One of the key tasks and preconditions for using smart metering systems is to find appropriate technical and legal solutions which safeguard protection of personal data as a fundamental right (…).

Member States and stakeholders should ensure, especially in the initial phase of the roll-out of smart meters, that smart metering system applications are monitored and that fundamental rights and freedoms of individuals are respected "

3. points of attention

Ongoing regulatory changes for smart grid & DP (p 19 WP 183)

- Current legal framework in privacy & DP
  (article 8 ECHR / Article 16 TFEU / Convention 108 / Directive 95/46/EC)

- Future legal framework in DP : Draft General Data protection regulation COM(2012) 11 final 25 january 2012 + Review of Convention 108

  http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm)

3. points of attention

- General low level of current compliance with DP

  examples :
  - access register of DSO's
  - Pro forma check of websites of energy providers
  - Function creep / (multisectoral) blacklisting

- Low level of awareness of DP

  Example 1 of incorrect assumption :
  DP does not applied on test data.

3. points of attention

Example 2 of incorrect assumption :

"technical data" vs. personal data

⇔

WP 136 and WP 183 (p8) : households and SME's are in scope (unique ID's with smart meters)

EC : smart metering allow processing of data, including personal data (Recital 6 Rec 2012/148/EC)

3. points of attention

- low level of (basic) transparancy

  examples :

  - websites of Suppliers, DSO's, regulators, ESCO's,…
  - letters to citizens have no DP content
  - low level of prior assessments by DPA s or prior notifications (often not applied in MS) (articles 18 and 20 DP Directive)
  - small meter displays in some MS (p 21 WP 183)

  ⇔ content of obligation to inform data subjects (article 10 DP Directive)

3. Points of attention

- Lack of PIA at EU level for EU energy packages

  ⇨ economic + also prior DP assessment as key requirement under Rec. 2012/148/EC

- Will Net Neutrality also be provided for smart grids ?

  Communication EC 19 april 2011 on open internet and net neutrality in Europe COM 2011 (222) final + Recital 7 Rec. 2012/148/EC

Choice to be made between "free market" management of smart grid data vs controlled market with neutral and impartial smart grid data management (balance of interests)

3. Points of attention

- Risk of unbalanced use of basis of legitimacy (article 7 DP Directive 95/46/EC)

  Examples :

  standard commercial practice is not “consent”

  unclarity in legal basis on “essential elements” of processing (article 8 ECHR)

4. Practical Recommendtations

- "prior checking" (article 20 DP Directive and 4-5 Rec 2012/148/EU)

  Different methods in MS :
  - Privacy impact assessment (new)
  - Also : regular consultation with DPA's (p 3 WP 183)
  - Also : function of DPO's and security counsellors ⇔ function of ICT manager

- Short & layered info and awareness raising
  - Clear DP statement on websites suppliers, DSO's, regulators (article 10 DP Directive)
  - Guidance for household management of smart meter data (FAQ / what to expect and to do…)

4. Practical Recommendtations

- logical link between key elements to be defined in laws (foreseeability of the law - article 8 ECHR)

Who	What	Why	Basis of Legitimacy
Qualification as "data controller" or "data processor" vs. DSO, suppliers, regulator,s ESCOs,…)	Type of data that is necessary (articles 6 & 7 DP Directive)	Definition of corresponding purposes / functionalities (article 6 1. (b) & (c) DP Directive)	Mainly law, also contract and consent (article 7 DP Directive)

4. Practical Recommendtations

- Guidance on correct use of the DP processing grounds (article 5 DP law – 8.2 DP Directive)
  - "DP consent" = right to object to all processing (the meter) and/or "push the button" consent for extra service applications ? ⇔ Traditional "commercial consent" in standard profile packages / standard in legal terms & conditions / lack of easy opt-out
  - legal basis / "public interest" must be of good quality / documented ⇔ only technical appendixes
  - contract only for the basic service (necessity criterium), and not for special services (ESCO,…)

4. Practical Recommendtations

- "Privacy by design" applied to smart meters (p16 WP 183 and articles 3 (d), 10-17 of Rec 2012/148/EU)

I.e.
Privacy principles built in the smart meters
Smart meters with high default level of DP

☝ not only security but also other principles such as data minimisation

4. Practical Recommendtations

- Examples of practical impact of Privacy By Design :
  - Frequency of sending data (proportionality principle)
  - Data storage period
  - Definition of access modalities / blocking for consumer / DSO user profiles …
  - Data storage location (home network)
  - Meaningful content of info visible on display
  - No "fishing expeditions" / wide scale processing of "all clients" for crime prevention or investigation purposes (p21 WP 183). Cf. SWIFT & ECHR Marper vs. UK case (data retention of DNA profiles). (availability of data creates demand)

4. Practical Recommendtations

- Combined levels of DP and Security Policy for every actor (level 1) + global assessment for sector (level 2)

Covered areas should include :

- Data retention policy (p 17 WP 183)
- "end to end" approach that includes household chain ⇔ "disclaimers approach"
- incident management (expect roll-out of broad security breach notification obligation in revision of DP Directive : add in regional laws vis à vis regulator / DPA?)
- Key technical and organisational issues (p 19 WP 183)

4. Practical Recommendtations

- Appropriate extra safeguards for higher risks (p 18 WP 183). Possibilities include
  - Official Opinion CBPL on projects of regional law
  - clearing house ("central information and communications hub")
  - code of conduct / consent / labels & privacy seals
  - competence sectoral commitee for regions (similar to federal sectoral commitee in article 36bis DP law) = mandatory checks prior to authorisation
  - Auditing and follow-up reporting made available upon request to regulator / DPA.

Every safeguard has +and - . One safeguard may not be full solution. Careful balance is key

5. Conclusion ?

- Balanced approach between both EU regulatory frameworks (no goldplating in one area)
- effective protection and positive approach to rights and obligations for users : real transparancy
- Prior DP Risk asessment (PIA) + continued follow-up & reporting available to DPA's & regulators
- More cooperation DPAs, regional supervisors & regulators
- Consequence of applicability of EU electronic communciations and DP legal framework on smart grids = Net neutrality also for smart grids ?
- Announced 2013-2016 : new DP impact assessment template of EC for smart meters + new regulatory DP framework

Thank you for your attention

Dieter VERHAEGHE

Legal Counsel