A new right requires guidance

Article 29 working party guidelines on data portability

Geoffrey Delcroix
Innovation and Foresight
CNIL
@geoffdelc
gdelcroix@cnil.fr
Independent Public Authority for personal data protection

- Protect personal data
- Accompany innovations
- Preserve civil liberties

**Advising and Regulating**
- 3,078 adopted decisions and deliberations
  - 190 authorisations
  - 145 requests for an opinion
- 1,976 transfer authorisations
- 54,000 simplified formalities

**Accompanying Compliance**
- 102,629 formality files
- 97 privacy seals delivered
- 14,734 declarations processed regarding video surveillance systems
- 316 biometric system authorisations

**Protecting Citizens**
- 7,703 complaints, of which 33% relate to prospecting
- 4,379 requests for access to police files, surveillance files, FICOA, etc.
- 410 complaints following the refusal of a request to be de-listed by search engines
- 7,909 inspections carried out

**Rendering Orders and Issuing Sanctions**
- 82 orders rendered
- 13 sanctions issued:
  - 4 financial sanctions
  - 9 warnings

**The CNIL Workforce**
- 195 jobs
  - 63% female
  - 37% male

@geoffdelc / @LINCnil
Missions

• Inform & Advise
  - Guidelines, tutorials, recommendations
  - Data protection officers trainings
  - Certifications, …

• Control & Sanctions
  - Prior formalities (authorizations, …)
  - Controls on site and online
  - Sanctions (financial, …)

Explore / Exchange / Experiment
Cahiers IP
A collection of publications around data ethics and digital trends

Privacy towards 2020
The body as a new connected object
Data, muses and frontiers of cultural creation
Share!
A media to share our analysis, ou points of view and tell the stories of our experiments

150 articles in 18 month (video, itw, )

#Drones  #Blockchain
#AI       #Robot
#SmartCity #Algorithms
#AutonomousCar #Ethics
#Design
Exchange and open CNIL to the world

- Conferences
- Workshops
- Demos

Espace LINC

@LINC.nil
Cookieviz
Visualization tool to measure the impact of cookies and other trackers during your own browsing.

L’Oracle du Net
An Interaction Design Project made “in residence LINC” by Victoria Duchatelle
A add-on for Chrome allowing users to explore the ways in which algorithms handle them.

Mobilitics
Understand the ecosystem of smartphones and lift the veil on these “black boxes” that are our smartphones.
How to monitor the progress and effectiveness of a right to be delisted request?
A tedious process if done by hand, but for which LINC has developed an open source browser add-on to automatize.

Does anonymisation make a dataset worthless? The data visualisations of our use case scenarios show that it does not necessarily jeopardise the quality of the results.

LINC looked into the core of Cnil’s activity by designing a data visualization of the GDPR.

@LINC.nil
More rights for your personal data!

1. Data to take away!
   I can get back the data I provided to an organisation or online-service and transmit those to other ones (social networks, Internet service provider, online streaming supplier, etc.)

2. Better transparency
   I know what is done with my data and it’s easier for me to exercise my rights.

3. Child protection
   Online services must obtain the parents’ consent before registering any child under 16 or less if provided by national laws.

4. One-stop-shop
   In case of problems with how my data is handled, I can contact my national data protection authority, whatever the country where the organisation is processing my data.

5. Bigger sanctions
   When infringing the regulation, the organisation at fault can be fined up to 20 000 000 € or 4% of its annual worldwide turnover.

6. Right to be forgotten
   I can ask search engines to delist a web page that affects my privacy negatively or ask a website to erase an information, under certain circumstances.

The European data protection regulation

After 4 years of discussions at the European Union level, a final draft of the data protection regulation has been released. It is expected to help Europe face the challenges of the digital age. The regulation will strengthen the citizens’ rights and provide them with real control over their personal data. It will offer a unified framework for companies and simplify the prior notification. The regulation will be formally ratified in early 2016 and will come into force in 2018 in all the Eu countries.
Right to data portability
2 misconceptions around GDPR data portability

• Seeing it as a mere extension of right of access «right of access under stéroïds»

• Confuse it with other competition / consumer laws related portability (as the one for phone number)
The right to data portability in a nutshell

- Basically, portability is about making the personal data "usable" directly by the individual or under his control and at his initiative beyond the control of the controller who collected it.

- It therefore offers people the opportunity to recover (part of) their "data" for their own purposes.

- Technically the concept of portability refers to being able to transfer data from one information system to another easily.

- Beyond the empowerment of the individual, portability must:
  Allow to avoid the effects of "lock in" (enclosure) of the consumers in a service to the detriment of the competing services and thus to facilitate the change of service provider ("switching")
  Encourage innovation by enabling data reuse in a new context without going through file interconnection.
Why does it matter?

For data subjects:
- Make the individual an actor of the use of data, not a simple "product"
- Reduce his/her dependency to data holders
- Allow him/her to switch service providers
- Enable him/her to adopt decentralized systems, even to self-host data and services.

For data controllers:
- Foster new services based on personal data without requiring them to collect them indirectly (via data broker…)
- Allow for the creation of a viable ecosystem of personal decentralized solutions (personal cloud, PIMS, …)
- Promote competition between similar services

For DPAs:
- Complementing the range of data subjects rights by a right having a different purpose than mere information / protection
- Embody the principle of informational self-determination concretely
- Give practical examples showing that the only solution for doing services with very high added value is not necessarily the centralization / concentration of personal data (the big data …)
Article 29 working party guidelines process

- **National consultation on cnil.fr**: June 2016
- **Results of cnil consultation**: Mid-July 2016
- **Data portability guidelines V1**: 12 December 2016
- **Data portability guidelines V2**: 2 April 2017
- **Consultation on Data portability guidelines V1**: Dec. 12 – Jan. 31
- **Fablab bxl**: 26 July 2016
WP 29 consultation
(December 2016 – February 2017)

Around 90 comments received, for a total of more than 600 pages...

Who?

Between a third and the half from business federations and lobbies (MS and EU)

Several DPAs and « privacy pros »

Around 20 companies in their own name

Several lawyers office (barrister)

Some individuals...

From?

Mainly EU member states

Several USA

1 NZ

3 Japan

Which sectors?

Banks

Telcos

Infosec / IT

Marketing, Ad

Software / digital players

Insurances

Who’s not there?
2 rights (and a half)

1. A right to receive data

2. right to transmit those data to another controller *without hindrance*  
   (and a right to direct transmission from RT1 to RT2 where technically feasible)
Portable data scope is limited

- A subset of a data processor data

What personal data must be included?

- Data actively and knowingly provided by the data subject
- Observed data provided by the data subject by virtue of the use of the service or the device

≠ inferred data and derived data are created by the data controller on the basis of the data “provided by the data subject”

- Consent
- Contract
  - Legal obligation
  - Protection of vital interests
  - Public interest mission
  - Legitimate interest
In practice

**Data subject** provides personal data in a structured, commonly used and machine-readable format.

**Data controller 1** provides a trust service provider.

**Trust service provider** stores data and helps to prove data subject identity as well as data integrity.

**Data controller 2** and **data subject** share with a controller authorized by the data subject.

**Personal storage** stores data.
Eligible data

1. Is it personal data concerning the data subject?
2. Is the data processing carried out by automated means?
3. Is the legal basis for data collection consent or contract?
4. Is it data provided by the data subject?
5. Would the portability adversely affect the rights and freedoms of others?

If yes to all, then the data are portable
Structured, commonly used and machine readable » + interoperability

- data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,…) along with useful metadata at the best possible level of granularity

WP29 strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.
RT providing portable data

« when technically feasible »
“Can occur when communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data.”

« without hindrance »
“any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller.

(...) fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardization or accreditation demands”
DPAs as part of a self data / MyData community

MyData is both an alternative vision and guiding technical principles for how we, as individuals, can have more control over the data trails we leave behind us in our everyday actions. The core idea is that we, you and I, should have an easy way to see where data about us goes, specify who can use it, and alter these decisions over time.

The MyData Global Network is a lightweight organisation to give structure and empower the movement that is growing from the international meetups and conferences and other interactions. The founding members are ambassadors for the movement and the action takes place in the local hubs around the world.

MesInfos

« If I (an organization) can use your data, you can too... however you please. » With this particular idea in mind, Ping and its partners launched the MesInfos pilot project in 2012.