GDPR
Rules and Impacts
For Registries

Overview

- The General Data Protection Regulation, (GDPR) is the new European reference document on the protection of personal data.
- It **strengthens** and **unifies** the protection of data for individuals in the European Union
- Its provisions will be directly applicable in all 28 Member States of the European Union as from **25 May 2018**.

Overview

Strengthens personal rights

- Strengthens consent and transparency
- Right to access one's own data
- Protection of minors under 16
- Right to compensation for damage
- By default protection as from data conception
- Etc.

Accountablity

- Removal of formalities but more accountablity
- Implementation of technical and organizational compliance measures
- Obligation for all Data Controllers (DC) to ensure the security of personal data and report personal data breaches
- Designation of a Data Protection Officer (DPO)

Shared Specific Responsabilities

- Identification of Data Controllers (DC) and Data Processors (DP)
- Supervision of data transfers outside the European Union
- In relation to individuals, everyone is responsible
- Graduated and strengthened penalities

Roles

RULES

- The role of each party must be defined in order to allow:
  - the right information to the persons concerned
  - the exercice of personal rights
  - the implementation of responsabilities

IMPACTS

- Clear identification of roles and processings

- For example (option on which Afnic is working) :
  - Registrars are responsible for the processing related to domain names services
  - The registry is responsible for the processing related to the technical resolution of domain names in the DNS
  - Both registries and registrars are recipient of personal data for their respective processings (both are data controllers)

Consent

RULES

- A personal data is, by nature, a confidential data
- The consent of a data subject remains one of the legal grounds for the processing of personal data under the GDPR

IMPACT

- Individuals contacts information (Registrant, Admin & Tech) will not be published in the Whois
- The restriction on the publication of personal data in the Whois will be implemented « by default » via EPP field : « Organization » (for past and future registrations)

Information & Transparency

RULES

- The consent of a data subject shall be *'freely given, specific, informed and unambiguous'*
- Importance of information and transparency towards registrants

IMPACT

- Before purchasing a domain name, the customer must be informed in a precise, clear and transparent manner of the processing of his/her data as a registrant:
  - Registry will provide a **Personal Data Policy** to help the transmission of information regarding its role and its processings.

- Registrars will be requested to comply with the GDPR (RRA)
  - By appointing a Representative for non-EU registrars
  - By designating a DPO or equivalent
  - By providing their customers with detailed, clear and transparent documentation on the processings and the exercise of personal rights

Right of access

RULES

- The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, **access to the personal data** and the following information (…)

IMPACT

- Implementation of a procedure (via an automated form) allowing the registrant to access its personal data upon request
- The form will lead the request on the proper processings (otherwise, the registry is supposed to answer on all its processings)

Personal Data disclosure

RULES

- Personal data protection principle must be balanced with the right to access information
- Which legal ground for such access?
  - IP right violation suspicion, court order, police investigation etc.

DATA ACCESS

- Access to Registrant information: on a case by case basis
  - Further to a decision in ex parte proceedings or legal requisition
  - On request from an authority (public enforcement agencies) authorised through their legal right of communication
  - By using a **form** available on the Registry website, depending on the status of the applicant or the ultimate purpose given by the applicant.

- The Registry will also provide a contact interface offering the possibility to third parties to communicate with a registrant.

Personal Data disclosure

FEW FIGURES (.fr)

- 420 requests per year on a basis of 3M domain names
- Answered in less that 1 day
- Less than 10 mn spent by request
- 70% of the requests come from law firm (IP issues)
- Others: Law enforcement agencies (Customs, Treasury, DPA, Judicial requisitions, Police etc.)

Right to Erasure

RULES

- Deletion of any personal data where such data is no longer necessary in relation to the purpose for which it was originally collected/processed

IMPACTS

- Definition of a precise rentention period for each pocessing
  - Active domain names: + 1 or 2 years after deletion of the domain name?
  - Escrow data ?
  - Other ?

Data transfer

RULES

- Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards, pursuant to Article 46 of the GDPR, relating to the transfer.

IMPACTS

- A clear and transparent Data Policy
- Non-EU Registrars will be requested to appoint a Representative in Europe
- Amendment of RRA provisions to ensure that non-EU registrars provide the same level of protection to EU citizens than GDPR
- ICANN?
- Escrow Agent?

Personal data breach notifications

RULES

- Each data controller and their subcontractors must ensure data security and, if necessary, carry out privacy impact assessments
- In case of personal data infringement, the data controller will notify the breach to its DPA within 72 hours, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons,
- The controller shall notify the person concerned of the fact that the infringement is likely to entail a high risk to his rights and freedoms

IMPACT

- The Registry and the Registrar will undertake, in order to meet these requirements (new provision in the RRA), to:
  - Have the necessary skills, resources and means
  - Inform the data subject in good time
  - Collaborate efficiently
  - Send all necessary information and documentation to Registry
- Implementation of a process at the Registry level for notifying DPA/Subject within time limit

GDPR

Rules and impacts

For Registries