The General Data Protection Regulation (GDPR)
Nordic Domain Name Days

Pontus Stenbeck, Hamilton Advokatbyrå
21 November 2017

Background and context

- Hamilton is a Stockholm-based full service law firm.
- Hamilton has been appointed by ICANN as independent third party expert to review certain issues regarding the processing of personal data within the gTLD ecosystem, in particular with regard to WHOIS, in light of the GDPR.
- Hamilton will issue a series of memorandums on the subject matter, of which the first was issued on 16 October 2017.

Controllers and processors

- Controller: ”the natural or legal person, public authority, agency or other body **which, alone or jointly with others, determines the purposes and means of the processing of personal data**” (art 4.7 GDPR).
- Processor: “means a natural or legal person, public authority, agency or other body **which processes personal data on behalf of the controller**” (art 4.8 GDPR).
- Not an obvious distinction within the gTLD ecosystem, as different parties may control certain parts of the processing.
- For the purposes of our legal assessment, ICANN, the registrars and the registries have been considered to be joint controllers.

Fundamental principles for compliance

- Lawfulness, fairness and transparency.
- Purpose limitation (specified, explicit and legitimate purposes, not incompatible purposes).
- Data minimisation (adequate, relevant and limited).
- Accuracy (accurate and, if reasonable, up to date – rectification, erasure)
- Storage limitation (not stored longer than necessary – cleansing).
- Integrity and confidentiality (appropriate security; protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).
- The controller shall be responsible for, and be able to demonstrate, compliance with GDPR (accountability).

Current processing

- Registrars and registries process a number of different types of personal data regarding registrants.
- The data is used for several different processing activities, such as:
  - invoicing, support, administration; and
  - publication in WHOIS directories.
- Personal data is currently processed by registrars and registries based on consent.
- For ccTLDs, national legislation in some EU member states (incl. Sweden) contain explicit requirements to obtain consent registering registrant data.

The challenges of consent under the GDPR

- ”Can’t we just continue to use consent as legal ground?”
- Consent must be freely given (art 4.11 GDPR) and possible to withdraw (art 7.3 GDPR).
- “When assessing whether consent is freely given, **utmost account** shall be taken of whether, inter alia, **the performance of a contract**, including the provision of a service, **is conditional on consent to the processing of personal data that is not necessary** for the performance of that contract.” (art 7.4 GDPR)
- Likely outcome → Not possible to condition the validity of a contract upon consent for a purpose which is not necessary for the performance of the contract.
- National law requirements for consents are likely to be removed/amended to suit the GDPR.

Alternative grounds for processing of registrant personal data

- Processing for performance of a contract (art 6.1 (b) GDPR).
- Based on legitimate interest (art 6.1 (f) GDPR).
- Based on consent for ”optional” purposes (art 6.1 (a) GDPR).

Performance of a contract

- Registrars should be able to rely on ”performance of contract” to process personal data which is necessary to perfom a contract with a data subject (e.g. a registrant who is also a natural person).
- Could include the following processing activities:
  - invoicing;
  - support;
  - other administration activities.

Legitimate interest

- The **legitimate interest of a controller or a third party** to be weighed against the **interests or fundamental rights and freedoms of the data subject**.
- Legitimate interest could likely be used as legal ground for certain processing activities such as:
  - administration activities where the data controller is not party to a contract with the registrant;
  - investigation of fraud, consumer deception, IP infringement etc;
  - law enforcement.
- Can legitimate interest be used to motivate making personal data publicly available through WHOIS directories?

Looking ahead, how to maintain public WHOIS directories

- Is it possible to maintain public WHOIS directories?
- Current view of DPAs and legislators seems to be that legitimate interest cannot be used to motivate publicly available WHOIS directories in their current form. Is this really the case?
- The future of WHOIS directories may be a combination of:
  - rephrasing, refining and clarifying the purposes for processing;
  - layered models of processing;
  - minimising the data to be made publicly available;
  - protecting data subject by use of opt-out options etc.
  - defining the need of public directories for domain names as a public interest?
- Discussion on principal level necessary.

Actions for compliance

- Actions on ICANN level will include:
  - principal assessment of legal grounds for processing;
  - update of agreements with registrars and registries.
- Actions on registrar and registry level will include:
  - review and update of agreements with registrants;
  - review and update of agreements with processors (such as resellers);
  - review and update of technical and organisational security measures.

Thanks for listening!

Pontus Stenbeck

Advokat | Senior associate

pontus.stenbeck@hamilton.se
+46 707 90 96 98

hamilton