geoTLD.group

GDPR
Recap, Impact and Solutions

October 2017

GDPR

Agenda

- GDPR Recap
- Registry Impact
- Registry Solutions

GDPR

Agenda

- **GDPR Recap**
- Registry Impact
- Registry Solutions

GDPR - Recap

- The **General Data Protection Regulation**, 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
- It aims at protecting European Union **citizens** and **residents worldwide**
- Its provisions will be directly applicable in all 28 Member States of the European Union as of **25 May 2018**

GDPR – Recap – Aims

Strengthen Personal Rights

- Data protection by design from inception
- Strengthened consent and transparency
- Right to access one's own data
- Protection of minors under 16
- Right to compensation for damage

Redefine Accountability

- Decreased formalities for increased accountability
- Designation of Data Protection Officers (DPO)
- Implementation of technical and organizational compliance measures
- Obligation to ensure personal data security and report breaches

Share Responsibilities

- Identification of roles:
  - Data Controllers (DC)
  - Data Processors (DP)
  - Data Subject (DS)
- Supervision of data transfer outside the European Union
- Collective responsibility over personal data
- International scope
- Graduated and strengthened penalties

GDPR – Recap – Definitions

Key Roles

- Data 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
- Data Processor
  natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- Data Subject
  an identified or identifiable natural person... EU citizen or resident

Fundamental Rights

- Information
- Access
- Rectification
- Erasure
- Restrict processing
- Data portability
- Objection

GDPR – Recap

ROLES & ACCOUNTABILITY

Data Controller, Data Processor, Data Subject

- Rule
  - Each role must be defined in order to allow
    - the right information to flow to the appropriate role
    - the implementation of responsibilities
    - the exercise of personal rights and responsibilities
  - GDPR replaces Administrative Formalities with Corporate Accountability
- Impact
  - Clear identification of roles
  - For each role, we need defined and documented processes to clarify and maintain accountability

GDPR – Recap

CONSENT

*any **freely given**, **specific**, **informed** and **unambiguous** indication [...] by a statement or **by a clear affirmative action**, signifies agreement to the processing of personal data [...]*

- Rule
  - Any data processing requires consent
  - Personal data is by nature confidential data
- Impact
  - No service without prior consent
  - No public access to personal data (even with consent)

GDPR – Recap

RIGHT OF ACCESS & RIGHT TO RECTIFY

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: [purpose, category of data, recipients, time span, rectification rights, rights to lodge complaints, 3rd party sources, automated decision making]

- Rule
  - Data Subjects can access any/all data processed and rectify it
  - True for data supplied by the DS, sourced from a 3rd party, or derived from the two previous
- Impact
  - Provide secure tiered access to private data (no public access)
  - Provide clear path to data rectification (using market standards where they exist)

GDPR – Recap

DISCLOSURE

The sharing of private data with legitimate 3rd parties

- Rule
  - Personal data protection principle must be balanced with the right to access information
  - GDPR establishes modalities for such access
    - Legal grounds: court orders, police investigation, IP right violation investigation, etc.
    - Means: only on a case by case basis, publicly available request interface, secure data exchange, fully traceable processes
- Impact
  - Replacement of current publicly available data interfaces, with request-based, individual, vetted and tracked data disclosures
  - Possibility to limit data disclosure, by forwarding direct communication from requestor to Data Subject

GDPR – Recap

DISCLOSURE

- Activity figures:
  - In .fr
    - 420 requests per year for 3M DUM
    - Requests are answered in less that 1 day
    - Less than 10 minutes spent by request
    - 70% of the requests come from law firm (IP issues)
    - Others: Law enforcement agencies (Customs, Treasury, DPA, Judicial requisitions, Police, etc.)
  - In .nl
    - 50-100 requests per year for 5M DUM
    - SIDN does offer full whois access to whitelisted Registrars, Law Enforcement and chosen IP Lawfirms
  - In .be
    - 5-10 requests per year for 1.5M DUM
  - In .cat
    - < 1 requests per year for 100k DUM

GDPR – Recap

ERASURE

"The right to be forgotten" or
the right to have personal data deleted

- Rule
  - Deletion of any personal data where such data is no longer necessary in relation to the purpose for which it was originally collected/processed
- Impact
  - Definition of a precise retention periods for each process in line with GDPR (Domain Lifecycle, Escrow, etc)
  - Definition of ad hoc processes where GDPR request delays are below agreed retention periods

GDPR – Recap

TRANSFER

[...] a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

- Rule
  - Article 45 – *A transfer of personal [...] may take place where the Commission has decided that the third country, a territory [...] ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.*
  - Article 46 – Where personal data is transferred to a third country or to an international organization without “Commission decision”, the data subject be informed of the appropriate safeguards, relating to the transfer.
- Impact
  - Ensure that all partners (data providers and data recipients) are defined and data sources and targets are adequately located
  - Ensure, where data is sent out of EU/GDPR purview, that local regulation offers GDPR protection
  - Present clear and transparent Data Policy with fully tracked data exchanges

GDPR – Recap

BREACH

Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Rule
  - 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
  - Controllers and Processors need
    - Necessary skills, resources and means to establish and maintain security protocols
    - Recorded evidence of security assessments, for themselves and data partners
    - Develop and document processes to inform DPAs, Data Subjects and partners in good time

GDPR

Agenda

- GDPR Recap
- **Registry Impact**
- Registry Solutions

GDPR – Impact

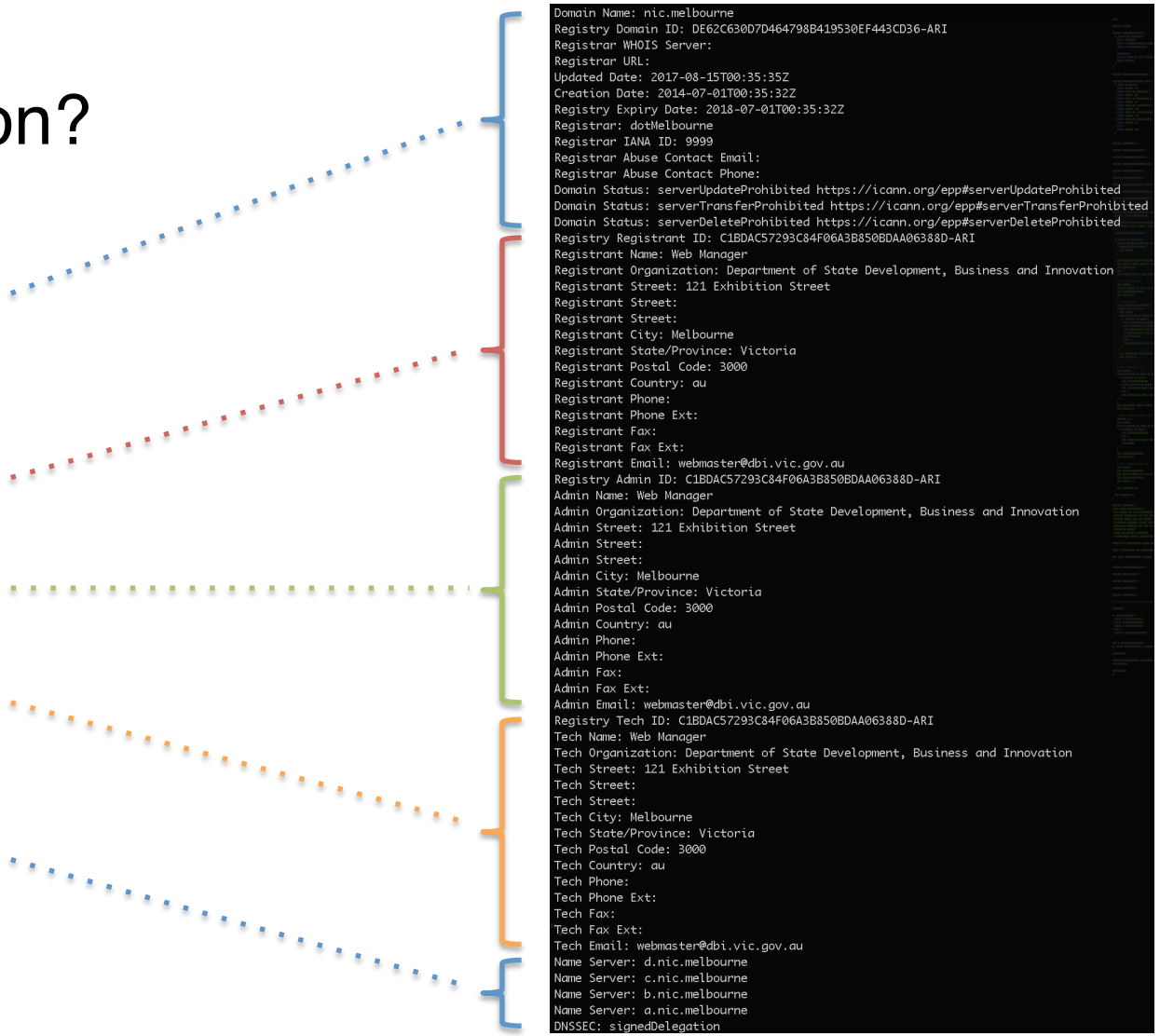
GDPR touches all aspects of private data management, but in the context of this presentation we will focus on services provided by Registries

- Whois and Escrow
  - What Information?
  - What is Public or Private?
  - Who should have Access?
- Other outputs and reports

GDPR – Impact – whois

What Information?

- Generic
- Registrant
- Admin
- Tech
- Generic



```
Domain Name: nic.melbourne
Registry Domain ID: DE62C630D7D464798B419530EF443CD36-ARI
Registrar WHOIS Server:
Registrar URL:
Updated Date: 2017-08-15T00:35:35Z
Creation Date: 2014-07-01T00:35:32Z
Registry Expiry Date: 2018-07-01T00:35:32Z
Registrar: dotMelbourne
Registrar IANA ID: 9999
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Registry Registrant ID: C1BDAC57293C84F06A3B850BDAA06388D-ARI
Registrant Name: Web Manager
Registrant Organization: Department of State Development, Business and Innovation
Registrant Street: 121 Exhibition Street
Registrant Street:
Registrant Street:
Registrant City: Melbourne
Registrant State/Province: Victoria
Registrant Postal Code: 3000
Registrant Country: au
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: webmaster@dbi.vic.gov.au
Registry Admin ID: C1BDAC57293C84F06A3B850BDAA06388D-ARI
Admin Name: Web Manager
Admin Organization: Department of State Development, Business and Innovation
Admin Street: 121 Exhibition Street
Admin Street:
Admin Street:
Admin City: Melbourne
Admin State/Province: Victoria
Admin Postal Code: 3000
Admin Country: au
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: webmaster@dbi.vic.gov.au
Registry Tech ID: C1BDAC57293C84F06A3B850BDAA06388D-ARI
Tech Name: Web Manager
Tech Organization: Department of State Development, Business and Innovation
Tech Street: 121 Exhibition Street
Tech Street:
Tech Street:
Tech City: Melbourne
Tech State/Province: Victoria
Tech Postal Code: 3000
Tech Country: au
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: webmaster@dbi.vic.gov.au
Name Server: d.nic.melbourne
Name Server: c.nic.melbourne
Name Server: b.nic.melbourne
Name Server: a.nic.melbourne
DNSSEC: signedDelegation
```

GDPR – Impact – whois

- What is Public?
  - Domain Name information
    - Domain name
    - Dates: Create, Update, Expiry
    - Status
    - Name Servers
    - DNSSEC
  - Registrar information

GDPR – Impact – whois

- What is Private?
  - Who?
    - Natural Persons
  - What?
    - Any contact details
  - From Where?
    - Everyone, if you are an EU entity
    - Just EU Citizens and Residents, if you are not

GDPR – Impact – whois

Information Types

Public Information

- Domain Name
- Registry Domain ID
- Registrar WHOIS Server
- Registrar URL
- Updated Date
- Creation Date
- Registry Expiry Date
- Registrar
- Registrar IANA ID
- Registrar Abuse Contact Email
- Registrar Abuse Contact Phone
- Domain Status
- ...
- Name Server
- DNSSEC

Potentially Private Information

- Registry *Contact* ID
- *Contact* Name
- *Contact* Organization
- *Contact* Street
- *Contact* City
- *Contact* State/Province
- *Contact* Postal Code
- *Contact* Country
- *Contact* Phone
- *Contact* Phone Ext
- *Contact* Fax
- *Contact* Fax Ext
- *Contact* Email

Contact = Registrant, Admin or Tech

GDPR – Impact – whois

Who gets access?

- Public Information is available to
  - Everyone
- Private Information is available to
  - Data Subjects
  - Authorities
  - 3rd Parties
  - Sponsoring Registrars

GDPR – Impact – Escrow

Escrow

- The same information as whois
  - Adding Reseller and Billing contacts if known
  - Escrow covers all Registry data where whois only shows current live domain data
- Submitted daily
  - Full or Partial deposits, Encrypted
- Send to a contracted partner

GDPR – Impact – Others

Audit your services

- BEROs typically offers
  - EPP, Reports
- BEROs may also offer
  - APIs, Escrow-like deposits, database dumps

- Ensure you know who has access to what and assess against your GDPR obligations

GDPR

Agenda

- GDPR Recap
- Registry Impact
- **Registry Solutions**

GDPR – Solutions

Data Processing
- Obtain/Maintain Consent
- Identify individuals to protect
- Data Update
- Data Retention

Whois
- Public Display
- Tiered Access

Escrow

Policy

All geoTLD group suggestions in Red

These result in our analysis of GDPR and the shared experience of AFNIC, CORE and SIDN

GDPR – Solutions – Processing

Obtain/Maintain Consent

- Define what consent means to you
  - Definition:
    freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

- Ensure Registrars obtain and renew Consent on terms that fit your needs, and pass it on for your record
  - Consent should be regularly renewed, we suggest yearly with whois data confirmation

GDPR – Solutions – Processing

Identify individuals to protect

- Natural Persons
  - Use of “Organization” or a new data point?
  - “Organization” can be used to identify businesses but only after proper explanations and consent is obtained
    Not to use assuming that all “Organization” are properly set
  - Which contact type? Registrant/Admin/Tech/Billing
  - All Contacts should to be considered separately
- Everyone or just EU Citizens and Residents
  - Use of “Country”? Can we make a distinction?
  - European Operators need to cover everyone
  - Non-European Operators may choose to do the same or require Contacts to identify themselves as Europeans

GDPR – Solutions – Processing

Data Update

- Keeping the Registry/Registrar model
  - All change requests should be directed to the Registrar
  - Direct Registry updates only in case of an unresponsive Registrar

- GDPR mandates update requests must be enacted within 1 month, well within industry practices

GDPR – Solutions – Processing

Data Retention

Retention of contact data no longer linked to existing domains

- Registry Data Retention must be reduced to GDPR acceptable level
  - European Registrars offer “jurisprudence”
  - We suggest aligning Registry requirements to the European Registrar waiver
- Keeping the Registry/Registrar model
  - Registrars should compelled via policy to regularly purge orphan contacts beyond retention
  - Registries should be able to purge contacts on behalf of Registrars only if unresponsive

GDPR – Solutions – Whois

Public Display

- Display Public Information
  - Domain name, Dates, Status, Registrar, Hosts, DNSSEC
- Treat Contacts individually
  - Where the Contact is a Natural Person
    - Replace all contact information by a disclaimer
  - Where the Contact is a Legal Entity
    - Maintain would display as is
  - Apply to whois.nic.tld and port 43

GDPR – Solutions – Whois

Public Display

- Edge Cases, private data in
  - Domain Names
    - Domain Names are public by essence, GDPR cannot apply
  - Registrar Information
    - Registrars must provide Abuse Contacts, these should be generic
  - Name Servers
    - As for Domain Names, public by essence
  - Registry *Contact* ID
    - Registry Registrant/Admin/Tech ID could be publicly displayed as long as throttling is in place to limit data farming

GDPR – Solutions – Whois

Tiered Access

- Concept
  - Allow different relevant entities and individuals to gain access to private data upon request
- Accountability
  - Keep track of all requests and answers
- Security
  - Put reasonable efforts in ensuring data is rightfully shared
- Response Time/Delays
  - Requests should be answered within 1 month

GDPR – Solutions – Whois

Tiered Access

- Establish processes to handle new requests
  - Requests should be received via a bespoke Web form or inbound email for traceability
  - Answers should be accountable and auditable
  - No requirement for immediacy, but some automation will ease traffic

GDPR – Solutions – Whois

Tiered Access – Example I

- Data Subjects
  - Must be able to request their own data
    - Contact details, linked domains and contact type, latest Escrow deposit, 3rd party Request for Info on them
  - Can request online
  - Partially Automated answers
    - For Contact details answer can be automated if sent to the registered email
    - More complex queries can be handled manually within 1 month

GDPR – Solutions – Whois

Tiered Access – Example II

- Authorities and Law Enforcement
  - Must be able to access any data
    - On a case by case basis: per domain or per contact
  - Can request online
    - Need to be able to justify their identity
  - Each demand should be verified
    - We can envisage whitelisted access to verified Authorities and Law Enforcement
  - Email forwarding can be offered
    - as a quicker/automated alternative to get in contact

GDPR – Solutions – Whois

Tiered Access – Example III

- 3rd Parties: IP Protection and others
  - May need to access data
    - On a case by case basis: per domain or per contact
  - Can request online
    - Need to be able to justify their identity and purpose
  - Each demand should be verified manually
  - Email forwarding can be offered
    - as a quicker/automated alternative to get in contact
- Registries are responsible for defining what legitimate requests are

GDPR – Solutions – Whois

Tiered Access – Example IV

- Registrars
  - Promote EPP Info
    - All sponsored information is accessible through EPP
  - Rationalize whois access
    - Public whois still offers key domain information
  - Registrars do not need to access non-sponsored contacts

GDPR – Solutions – Escrow

Currently by contract

- All Registry data is Escrowed
- Daily updates & Full deposit from time to time
- Retention is 10 years
- In principle, no one but ICANN/EBERO has access, but some Escrow providers use data

❑We only need to be able to retrieve current operational data

- Multiple backups may be needed to ensure clean available data

GDPR – Solutions – Escrow

For GDPR

- Only current operational data is Escrowed
- Daily updates & Full deposit weekly/monthly
- Retention down to 1 year
- No one but ICANN/EBERO has access

❑We ensure

- Multiple full deposits of backup
- Old data is only maintained for a short time
- Downstream processing is limited to EBERO

GDPR – Solutions

Policy

- All data points must be reviewed limiting to what is needed
  - To provide the service
  - To run targeted ancillary services (reports, specific stats, marketing campaigns, etc.)
  - To comply with contractual obligations (where these are not directly in conflict with GDPR)
- All data relevant policies must be
  - Reviewed: data collection, storage, analysis, exchanges, etc
  - Amended: aligned with GDPR requirements
  - Disseminated: to all parties including Registrants via their Registrar
  - Approved: by consent from Data Subjects, by contract for other partners

Disclaimer

This presentation does not constitute advice, legal or other.

It represents our experience and the knowledge we gathered in preparing for GDPR. We thank AFNIC, CORE and SIDN for their assistance.

All the information shared is in our opinion accurate, but should be verified in your context by trained professionals (legal and others).