Roles and Responsibilities Discussion Group

9 November 2020

CPH Comments on DPA: <https://docs.google.com/document/d/1nJADGeDZNSU1R5okQzlMBLQpJggufyxeHGACWpLnLBA/edit>

**5: Security of Personal Registration Data**

* 5.3.1: ok, as want policy on encryption.
* Worry 5.1.2 saying something should always be encrypted. Too much operational detail and things change over time
* Suggested alternative text: ‘Taking into account the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, each party shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, such as:’ and include some examples could just include encryption
* Want ICANN to be required to do some things.  ICANN should not audit CPs security systems, should be the other way round

**6: Security Breach notification**

* Updated terminology
* 6.1: CPH trying to limit scope for what required notification, so that not every breach requires notification to ICANN or the other party.  This language has been dropped
* 24hrs for notification is not ok
* Not breaching contract by not telling ICANN.
* Language is broader.  Understand breach vs incident.  Should be all data, not just required
* GDPR requires notice only if it’s likely to risk the rights and freedoms of natural persons (ie registrants).  There’s no reference to balancing activity
* Relying on ICANN to define the nature of a breach
* Section is not about notification to authorities but between the parties, doesn’t require public disclosure, so clause is for CPs protection/benefit. Not all breaches occurring to CPs will need to be notified, but in all cases CPs should be notified of breach found at ICANN’s end
* ICANN have 24hrs to notify CPs and CPs have 72hrs to go to authorities. Article 33.1, says not more than 72hrs to provide notice
* In other industries, breaches are preferred to be kept quiet, so should aim to minimize disclosure of breaches as it impacts the industry. Don’t want paper trail of privacy breach that may culminate in a GDPR breach.
* If something goes wrong, ICANN will go to CPs before the authorities and would prefer that.  If it’s a true data breach, is too late anyway
* 6.2: Ok with email notification, but not regular mail.  Should go to designated privacy contact
* Concern with use of NSp as an example as It operates in real time and if that’s the choice of mechanism what happens if it can’t be used.
* 6.4: If appropriately scope the section for situations where ICNN has experienced a breach that impacts a CPs customers, this clause is important and ICANN should not make any announcement without talking to CPs first.  Any breach notification requiring Data Protection Authority is not in scope.
* Should be mutual, not just the registry
* Don’t understand purpose of the clause.  A breach would involve registration data, so an obligation to notify registrants/registrars.  If could rely on CPs to follow data protection laws wouldn’t need this, but now DPA is carving out the requirement
* Matt to redraft tightening the scope
* 6.5: the indemnification clause in RA is one way, but it’s not appropriate in context of this agreement.  Otherwise registries will be on the hook to indemnify ICANN, but there’s no reciprocal obligation.  Know from SSAD discussion where ICANN stands on indemnification.  Will come back to it.  See this as a back door to ICANN not taking any responsibility

**7: Data Subject Rights**

* Has been discussed at length and the section is edited for the sake of editing.  Was supposed to be about cooperation, but now just putting obligations on CPs
* 7.3/4: Don’t make sense.  Needless clause, as it’s additional to GDPR requirements
* Need some cooperation.  If ICANN receive a request for data they don’t have, would be good for them to forward it or direct registrant to the impacted CPs
* Should not be assistance between parties.  If the CP has no data, should only say that
* Should go back to original language.  Having a general cooperation clause should be discussed as seems to be important to ICANN.  Can be confusing for registrants to know their relationship with parties.

**8: Data Retention and Deletion**

* Put back original language as it’s cleaner

**9: Processing of Communications**(proposed change to Cooperation – Resolution of disputes)

* As with section 7, same question of whether need to shift data request to another party.  No requirement to do so under GDPR.  Tied into accountability which is only enforceable by an EU authority, and is not applicable data subject requests
* Normal to see this type of language on cooperation in a DPA.  More a standard clause, than GDPR related.  Think intended for case where a regulatory authority is involved, and what happens to appropriately respond
* Why should a registrar cooperate with registry, it should not be an obligation to assist a registry to meet their RA requirements and GDPR duties.  Registrars will inevitably be required to provide assistance and if not, there will be a complaint to ICANN
* This is not about being abusive or creating extra work for registrars

**10: Compliance audits**

* Whole section should be deleted
* Think ICANN want that implementation can be audited
* Should be narrowed and renamed as it’s a reciprocal agreement and should be mutual work
* Should decide what CPs are comfortable with first – for example, both be self-certified, certified by independent party, have more onus on ICANN for smaller CPs who don’t have the resources, etc
* Need to be clear what is meant by audit
* If going to audit, should be mutual and must only be in context of standard compliance audit
* Don’t like annual report
* Concern about ICANN getting an additional hook to catch CPs.  Could model after code of conduct

**11: Limitation of liability**

* Frees ICANN and CPs from complying from any terms of the agreement unless they are subject to GDPR, which defeats the purpose.  Supposed to impose GDPR responsibilities on CPs and ICANN.  No point to their being a waiver.
* Not sure what the clause is saying.  There’s ambiguity about be subject of liability
* Whole section to be flagged to discuss how liability should be addressed in the DPA.  Want to understand what the agreement is
* Don’t think we can have a clause that allows registries to have an out to apply data processing obligations
* DPA required because there’s processing of shared data, not only for GDPR
* Matt to redraft

**12: Entire Agreement: Priority**

* 12.1 Would like to leave open the door to an actual DPA
* Flag section for discussion as don’t understand
* Can say prefer it being a DPA that’s appended
* No other specification has a clause like this

**13: Breach: Termination**

* 13.1: Issue again being one way rather than mutual.  Beth to redraft
* 13.3: if terminated, does the underlying means of transfer end as well?

**14: Confidentiality**

* Have not seen in a DPA before
* Does not have to labeled. Can be broadened, in line with 7.5
* Not sure if it’s the same with RAA (Serena to check)

**Next Meeting**

* Meeting on Friday to be CPH only and will meet again with ICANN the week after